The regulation of privacy on cloud computing services in terms of the Protection of Personal Information Act 4 of 2013

A thesis submitted in fulfilment of the
requirements for the degree of

MASTER OF LAWS

at the

RHODES UNIVERSITY
Faculty of Law

by

MTHUTHUKISI MALAHLEKA

SUPERVISOR: MS TN MASHININI

https://orcid.org/**0000-0003-4564-8559**

DECEMBER 2021

Declaration of Originality

1. I, **Mthuthukisi Malahleka**, know that "plagiarism" means using another person's work and ideas without proper acknowledgement, and pretending that it is one's own. I know that plagiarism not only includes verbatim copying, but also the extensive (albeit paraphrased) use of another person's ideas without proper acknowledgement. I know that plagiarism covers this sort of use of material found in court judgments, textbooks, journal articles AND on the Internet.

2. I am aware of the University and the Law Faculty's policies on plagiarism as set out in the Faculty's *Handbook*.

3. I acknowledge and understand that plagiarism is wrong, and that it constitutes academic theft.

4. I understand that my research must be accurately referenced. I have followed the rules and conventions concerning referencing as set out in the Law Faculty's *Handbook*. I accept that merely putting a reference next to the copied words of others is not sufficient to avoid a charge of plagiarism, and that I understand the writing conventions applicable to using direct quotes and quotation marks.

5. This thesis is my own work.

6. I have not allowed, nor will I in the future allow, anyone to copy my work with the intention of passing it off as his or her own work. I also accept that submitting identical work to someone else constitutes a form of plagiarism.

Signed……M Malahleka……...

Acknowledgements

First and foremost, I would like to praise the Lord Almighty for holding my hand and walking this journey with me. The same God made it possible to be accepted by Rhodes University and get an amazing supervisor for my LLM research thesis. Secondly, I would like to thank my supervisor Ms N Mashinini for her help throughout my LLM research. I was fortunate to be supported by a brilliant academic, strong, professional, and empathetic woman. Ms Mashinini provided me with insightful academic feedback and helped me complete the thesis. Her emphasis on the importance of "finding my voice within my research and speaking to the reader through my research content by creating a clear "goldern thread"" will stay in my mind forever. Her insightful feedback has helped me significantly understand how to conduct an entire thesis research study at the LLM level. It might seem like our time together ended soon. However, this marks the beginning of a new academic relationship in the ICT law space. I look forward to working with her on conducting more research studies and publishing journals and articles, who knows, even a textbook!

Thirdly, a big shout out to my two adorable boys Unathi and Luyanda. You are the reason I wake up every day with a smile on my face and look forward to each day with a positive mind to work hard so that I can give you what I never had; a good life. At some point, I felt like giving up, but when I think of you two, I would wake up in the middle of the night and start afresh from where I left "giving up has never been an option" *ngane zami*. I am so proud of you; my boys and Daddy love you so much; I find myself falling in love with you two even more profound every day. Lastly, I would like to thank my Mother, Wasithanda and my father, Ntando, for taking care of my two boys in my absence and for all the love you give them. I love you both so much. I am not forgetting my lovely sister Ndi raising and falling with me and taking care of my boys. It has been indeed a roller coaster, but we made it, sister! I love you; stay blessed. To the rest of my family, I love you all; God Bless you. *Lanini!*

Abstract

There is a relatively new development in Information Technology (IT) space known as cloud computing, software and service delivered remotely through the Internet without installing software on a computer. Cloud computing has quickly gathered steam as one of the most prominent topics in IT, and indeed within the business sector as a whole. Cloud computing is one such development associated with opportunities and benefits, especially in the commercial sector.

Due to the development of IT and many businesses adopting e-commerce business-related strategies, cloud computing has revolutionised how personal information is processed. The advent of cloud computing as a mechanism to process personal information has brought many legal challenges for protecting the right to privacy enshrined under section 14 of the South African Constitution, which is a vulnerable part of one's personality right. The right to privacy has long been protected even before adopting the Constitution under the common law of delict (*actio iniuriarumn*).

As the adoption rate of cloud computing services by businesses continues to increase, the legal considerations and risks become more prevalent. The lawmakers struggle to keep pace with the rapidly changing technological advancements, at least for now. Both the common law and the Constitution could not address all the legal aspects of data protection and the adoption of cloud computing services hence the promulgation of the Protection of Personal Information Act 4 of 2013 (POPI Act). The POPI Act's main objective is to protect the personal information of both natural and juristic persons. Personal information about an individual forms part of privacy. Unlawful processing of such personal information is a violation of the right to privacy of an individual. It is now widely recognised that the unregulated processing of personal information significantly impacts fundamental human rights like privacy, personality, and autonomy.

A close analysis of cloud computing regulation is necessary, as legal protection mechanisms must safeguard the processing of personal information and establish extraterritorial jurisdiction to regulate the use of cloud computing within national

legislation as cloud computing provides a transnational characteristic on the cross-border flow of personal information.

In this thesis, a question is asked on whether the current data protection laws in South Africa on protecting the right to privacy in the cloud computing services context are adequate. The analysis will determine whether the overlaps between these pieces of data protection laws are competent to deal with the ever-increasing threats on the right to privacy and if they meet the international data protection standards set by the European Union's General Data Protection Regulation (GDPR). The research seeks to analyse and reveal the shortcomings under the Constitution and the common law that led to adopting the POPI Act by studying the regulation of cloud computing services.

This analysis will determine the shortcomings of the POPI Act as well in the context of cloud computing. The research will then follow a comparative analysis of the POPI Act and the GDPR to determine the application of the GDPR on international data breaches and compare its provisions with the POPI Act in the context of cloud computing. Finally, the research will address the question as to whether a multi-faceted approach, which includes a Model Law on cloud computing, would be an appropriate starting point setting out requirements for the use of this technology can be sufficient in protecting data subjects. And as cloud computing risks are not only a national but also a global problem, South Africa needs to look at the option of entering into mutual agreements with other countries and organisations to regulate cloud computing at an international level.

Keywords: Protection of Personal Information Act (POPI Act), cloud computing, data protection, personal information, privacy, General Data Protection Regulation (GDPR)

Table of Contents

Acronyms and Abbreviations

ACD	Amazon Cloud Drive
ACM	Association of Computing Machinery
Acta Juridica	University of Cape Town's Law Faculty's Law Journal
AD	Appellant Division Reports
AEPD	Spanish Data Protection Agency
AfriNIC	African Network Information Centre
AI	Artificial Intelligence
AIDS	Acquired Immune Deficiency Syndrome
AJ	Acting Judge
AMLR	Auditory Middle Latency Responses
APNIC	Asian Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
BCLR	Butterworths Constitutional Law Reports
BILETA	British and Irish Education Technology Association
Bol.Fac.Direito.U.Coimbra	Boletim da Faculdade de Direito Universidate de Coimbra
BSASA	Business Software Alliance South Africa
CC	Constitutional Court
CE	Council of Europe
CFR	Charter of Fundamental Rights
CILSA	Comparative and International Law Journal of South Africa

CJ	Chief Justice
CJHR	Canadian Journal of Human Rights
CJIL	Chicago Journal of International Law
CLOUDA	Clarifying Lawful Overseas Use of Data Act
CLR	Commonwealth Law Reports
CLSR	Computer Law and Security Review
CNIL	Commission nationale de l'informatique et des libertés
CPD	Cape of Good Hope Provincial Division Report
CSO	Community Security Organisation
Cybaris INTELL. PROP. L. REV.	Cybaris Intellectual Property Law Review
DBCLJ	DePaul Bus and Commercial Law Journal
De Jure	De Jure
DEF CON	DEFense CONdition
DPA	Data Processing Agreement
DPA	Data Protection Authority
DR	De Rebus South African Attorney Journal
DUBLIN U. L.J.	Dublin University Law Journal
EC	European Community
ECA	Electronic Communications Act
ECC	Elastic Compute Cloud
EDPB	European Data Protection Board
ELEC.L. J	Potchefstroom Electronic Law Journal
Era Forum	Journal of the Academy of European Law

ETS	Establishment Number
EU	European Union
EUR. DATA PROT. L. Rev	European Data Protection Law Review
GATS	General Agreement on Trade and Services
GB	Gigabite
GDPR	General Data Protection Regulation
GroJIL	Groningen Journal of International Law
GSJ	Global Scientific Journal
HC	High Court
HCA	High Court of Australia
HCLT	Centre of Law and Technology
HIV	Human Immune Virus
IaaS	Infrastructure as a Service
IBERJ	International Business and Economics Research Journal
IBM	International Business Machines Corporation
ICANN	International Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology
IDPL	International Data Privacy Law
IEEE	Institute of Electrical and Electronics Engineers
IITA	Indian Information Technology Act

INT'l L. News	International News
INT'L LAW REVIEW	International Law Review
IP	Internet Protocol
IR	Information Regulator
ISACA	Information System Audit and Control Association
IT	Information Technology
IVTO	International Vocational Training Organisation
J	Judge
J. INTELL. PROP. INFO. TECH. & ELEC. COM. L.	Journal of Intellectual Property, Information Technology and E-commerce
J. INTERNET L	Journal of Internet Law
JBM	Journal of Business Management
JJ	Judges Journal
JMJITPL	John Marshall Journal of Information Technology and Privacy Law
JPA	Journal of Public Administration
JURIDICA INT'L	Juridica International Law Review
LICRA	La Ligue Contre le Racisme et L'Antisemitism
LJHSE	Law Journal of Higher School of Economics
LLD	Doctor of Laws
MEC	Member of Executive Council
MLA	Mutual Legal Assistance
NCA	National Credit Act

NIST	National Institute of Science and Technology
NUALS	National University of Advanced Legal Studies
NYULR	New York University Law Review
OECD	Organisation for Economic Co-operation and Development
PaaS	Platform as a Service
PAIA	Promotion of Access to Information Act
PCIJ	Permanent Court of International Justice
PELJ	Potchefstroom Electronic Law Journal
Ph.D	Doctor of Philosophy
PIPEDA	Personal Information Protection and Electronic Documents Act
POPI	Protection of Personal Information Act
RIPE-NCC	Reseaux IP Europeans Network Coordination Centre
RIR	Regional Internet Registries
SA	South Africa
SaaS	Software as a Service
SACJ	South African Computer Journal
SALJ	South African Law Journal
SALRC	South African Law Reform Commission
Santa CLARA HIGH TECH. L. J.	Santa Clara Hight Technology Law Journal
SAPS	South African Police Services
SCA	Stored Communication Act

SCA	Supreme Court of Appeal
SCLR	Santa Clara Law Review
SCV	Supreme Court of Victoria
Seattle U. L. REV.	Seattle University Law Review
SJLS	Singapore Journal of Legal Studies
SLA	Service Level Agreement
STLR	Stanford and Technology Law Review
T	Transvaal
TECLF	Tulane European and Civil Law Forum
TGI	Tribunal de Grande Instance
THRHR	Tydskrif vir Hedendaagse Romeins-Hollandse Reg
TILEC	Tilburg Law and Economics Centre
TILJ	Texas International Law Journal
TSAR	Tydskrif vir die Suid-Afrikaanse Reg (Journal of South African Law)
UCT	University of Cape Town
UEJF	Union des Etudiants Juifs de France
UKZN	University of Kwa-Zulu Natal
UN	United Nations
UNHRC	United Nations Human Rights Council
UNISA	University of South Africa
USA	United States of America
W	Decision of the Witwatersrand Local Division

WC	Western Cape
WJLTA	Washington Journal of Law Technology and Arts
WTO	World Trade Organisation
ZA	Zuid Afrika

Chapter 1: Introduction

1.1 Introduction

The processing of personal information is not a new phenomenon.[1] Record-keeping on individuals is as old as civilisation itself. However, the advent of computers during the 1950s played a crucial part in making personal information a valuable commodity. Computer technology influenced both the quantity and the quality of processing of such information.[2] Computers can quickly store vast amounts of information, cheaply and for almost indefinite periods.[3] The advent of better and faster computer chips and processor speed has grown exponentially in the past decades. The demand for computing power has also grown within the global community.[4]

There is a relatively new development in the Information Technology (IT) space known as cloud computing. The word "cloud" is used as a metaphor for the "ethereal Internet" and the virtual platform that it provides.[5] An important aspect of cloud computing technology is not being confused with the Internet, an open-access web-based platform. Most cloud computing services are privately owned and offer access to metered IT services. There is also a new increasing trend of providing cloud computing services to the public.[6] Cloud computing services are delivered by way of an IT platform for software and other supplementary applications provided via remote file servers across the Internet on a requirements basis.[7]

[1] J Neethling *et al Neethling on Personality Rights* 2nd Edition (2019) 365.
[2] A Roos "Explaining the International Backdrop and Evaluating the Current South African Position" (2007) 124 *SALJ* 2 at 401.
[3] Roos 2007 *SALJ* 401 and Neethling *et al Neethling on Personality Rights* 366 to 367.
[4] *Ibid.*
[5] D A Couillard "Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing" (2009) 93 *Minnesota Law Review* 2205 at 2205 to 2216.
[6] A P Jackson *Legal Concerns Arising from the use of Cloud Technologies* (LLD Thesis, UP,2017) 17.
[7] T D Martin "Hey! You! Get off my Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security and Property in Cloud Computing" (2010) *Journal of the Patent & Trademark Office Society Selected Works* https://works.bepress.com (Accessed 21 March 2020) and Neethling *et al Neethling on Personality Rights* 367.

1.2 Cloud computing as a mechanism to process personal information

Cloud computing is a system by which individuals can access computing power remotely by processing data on centralised servers, as if in a "cloud".[8] This is the practice of using a network of remote servers hosted on the internet to process data.[9] Cloud computing links remote computers to access remote data storage and computation services from servers located anywhere in the world.[10]

Cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in response to demand.[11] The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling convenient and on-demand network access to a shared pool of configurable computing resources.[12] Such resources include networks, servers, storage, applications and services.[13] These configurations can be rapidly provisioned and released with minimal management effort or service provider interaction.[14]

Furthermore, Cloud computing is a mechanism that consists of a set of technologies and service models.[15] It also involves the cross-border transfer of personal information

[8] V Narayanan "Harnessing the Cloud: International Law Implications of Cloud-Computing*"* (2012) 12 *Chicago Journal of International Law* 783 at 785.

[9] D P Van der Merwe *et al Information and Communications Technology Law* 2nd Edition (2016) 366.

[10] Narayanan 2012 *Chicago Journal of International Law* 784.

[11] C Sullivan "Protecting Digital Identity in the Cloud: Regulating Cross Border Data Disclosure" (2014) 30 *Computer Law & Security Review* 137 at 138, H B Jr Dixon "Cloud Computing" (2012) 51(2) *Judges Journal* 36, B Smith "Cloud computing for business and society" (2010) *Brookings Institution* http://www.brookings.edu / (Accessed 07 April 2020) and M Peihani "Financial Regulation and Disruptive Technologies: The Case of Cloud Computing in Singapore" (2017) *Singapore Journal of Legal Studies* 77.

[12] P Mell and T Grance "The NIST Definition of Cloud Computing" (2011) *U.S. Dept. of Commerce National Institute of Standards and Tech Special Publication No. 800-145, The NIST* 2 http://csrc.nist.gov/publications/nistpubs/800-145/SP800- 145.pdf (Accessed 19 April 2020) and J Hage and J S Brown "Cloud Computing - Storms on the Horizon" *Deloitte Centre for the Edge* 2 http://www.johnseelybrown.com/cloudcomputingdisruption.pdf (Accessed 05 July 2020).

[13] *Ibid*.

[14] *Ibid*, Sullivan 2014 *Computer Law and Security Review* 138, A L D Pereira "Cloud Computing" (2017) 93 *Bol. Fac. Direito U. Coimbra* 89 and R Berry and M Reisman "Policy Challenges of Cross-Border Cloud Computing" (2012) 4 *Journal of International Commerce and Economics* 1 at 2.

[15] Council of Europe Article 29 Data Protection Working Party Opinion 01037/12/EN WP 196 (2012) 4 and P Sahoo and T Jaiswal "Cloud Computing and its Legalities in India" (2014) 4 *Nirma University Law Journal* 65.

across various jurisdictions[16] for multiple clients across the globe.[17] It entails storing information on various cloud computing service provider servers instead of storing data and software on the client's hard drive. Examples of these cloud computing services include Google Drive operated by Google, iCloud operated by Apple and Microsoft Azure.

1.3 Problem statement

There are significant benefits and opportunities associated with this computing model,[18] these will be highlighted below in the subsequent headings and chapters. Cloud computing is quickly gathering steam as one of the most prominent emerging IT solution in many businesses at large. Managers and business owners are considering alternative ways to move to cloud computing in various sectors that can potentially benefit their organisations. For example, the use of e-commerce and online shopping.

Despite this, there is still a significant lack of understanding of cloud computing platforms' benefits and inner workings. Concisely put, the days in which small businesses were forced to invest in costly IT infrastructure to accommodate growth have significantly shifted and become better and less expensive. Today, cloud computing is offering businesses a simple answer to the challenge of IT scalability through hosted environments that can be provisioned easily.

Population growth and technological innovations have made the processing of personal information ubiquitous in everyday life.[19] Some individuals share personal information voluntarily on social networks.[20] Other individuals provide businesses and

[16] B Preston "Customers Fire a Few Shots at Cloud Computing" (16 June 2008) *INFO WK* 52 http://www.informationweek.com/news/services/data/ show Article jhtml? Article lD =208403766 (Accessed 04 April 2020).

[17] Van der Merwe *et al ICT Law* 367 and R H Carpenter Jr "Walking from Cloud to Cloud: The Portability Issue in Cloud Computing" (2010) 6 *Washington Journal of Law, Technology & Arts* 1 at 2.

[18] Article 29 *Data Protection Working Party* 01037/12/EN WP 196 Opinion 5/2012 on Cloud Computing (2012) 4 http://ec.europa.eu/justice/data-protection/index_en.htm (Accessed 21 March 2020) and Neethling *et al Neethling on Personality Rights* 367.

[19] Van der Merwe *et al ICT Law* 363 and Neethling *et al Neethling on Personality Rights* 366.

[20] Neethling *et al Neethling on Personality Rights* 366.

financial institutions with personal information for credit applications, purchases, employment and medical reasons.[21]

The development of Information and Communications Technology (ICT) has changed how personal information is processed across the globe.[22] Public and private bodies have shifted from the paper-based approach of processing personal information to electronically processing personal information through computerised systems.[23] Environmental and efficiency reasons have also necessitated this shift.

1.3.1 Challenges of cloud computing portability

However, as much as cloud computing can provide so many advantages and benefits, it brings new challenges for data privacy law.[24] The first significant problem encountered in cloud computing is that it is difficult to link the stored information in the "cloud" to the responsible party who processed that personal information.[25] Centralised servers process personal information from clients residing in many different countries. In contrast, the location of their servers is in a few countries only.[26]

A cloud service client loses exclusive control over the personal data they upload on the cloud because the information is being processed and stored on servers. The service client will not always have enough information on how data is processed, where it is accessed and by whom it is accessed.[27] Furthermore, if the cloud service client is not in control of the data, they may also not know all the possible security risks that their information is subject to. Therefore, it may not be possible for the client to ensure that the required security measures are in place.[28]

---

[21] Van der Merwe *et al ICT Law* 364 and Neethling *et al Neethling on Personality Rights* 366.
[22] N Olorunju "Security: The Protection of Personal Information in the Health Care System" (2019) 54 *Journal of Public Administration* 363 and Neethling *et al Neethling on Personality Rights* 366.
[23] Van der Merwe *et al ICT Law* 364.
[24] Van der Merwe *et al ICT Law* 367, Neethling *et al Neethling on Personality Rights* 367 and W K Hon, C Millard and I Walden "The Problem of 'Personal Data' in Cloud Computing: What Information is Regulated? The Cloud of Unknowing" (2011) 1(4) *IDPL* 211.
[25] Hon 2011 *IDPL* 228.
[26] Narayanan 2012 *Chicago Journal of International Law* 785. For example, Google only has data servers located in some parts of the Americas, Asia and Europe, but not Africa, while many of its users are in Arica as well https://www.google.com/about/datacenters/inside/locations/ (Accessed on 30 March 2020).
[27] Van der Merwe *et al ICT Law* 367.
[28] *Ibid.*

1.3.2 The threat of data security risks

The individual and corporate users of cloud computing are exposed to the risk of data loss and violations of privacy.[29] Even the most advanced computer systems are subject to security risks.[30] Furthermore, the lack of control over the hardware of cloud computing services poses risks such as hacking, data breaches, data leaks, and the interception of data.[31] These risks include unauthorized persons gaining access to internal systems and databases through an organisation's computer networks and then subsequently, to data subjects' personal information. These unauthorised system access techniques are executed through web applications such as spoofing[32] and phishing.[33]

These risks make it imperative that both public and private bodies safeguard the personal information that they process by, for example, implementing strong firewalls, data encryption, policies and procedures.[34] Some of the risks that emanate from the use of cloud computing are multi-tenancy, which refers to the ability to run multiple application users on a shared infrastructure. This facilitates economies of large scale by saving on the per-user cost of operations.

Human error and a lack of proper understanding among cloud computing users can lead to severe implications exposing personal information to cybercriminals.[35] However, South Africa has adopted the Cybercrimes Act 19 of 2020 (Cybercrimes

---

[29] Narayanan 2012 Chicago *Journal of International Law* 787 and Neethling *et al Neethling on Personality Rights* 366.

[30] R von Solms and M Viljoen "Cloud Computing Service Value: A Message to the Board*"* (2012) 43(4) *Journal of Business Management* 73 at 77.

[31] T Peterson "Cloudy with a Chance of Waiver: How Cloud Computing Complicates the Attorney-Client Privilege" (2012) 46 *J Marshall L Rev* 383 at 390 and Neethling *et al Neethling on Personality Rights* 366.

[32] Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. ... Spoofing is often the way a bad actor gains access to execute a more extensive cyber-attack such as an advanced persistent threat or a man-in-the-middle attack Forcepoint https://www.forcepoint.com/cyber-edu/spoofing (Accessed 21 February 2022).

[33] Phishing is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware. Wikipedia https://en.wikipedia.org/wiki/Phishing (Accessed 21 February 2022).

[34] Section 19 of the Protection of Personal Information Act.

[35] R Sony "Implications of Cloud Computing for Personal Data Protection and Privacy in the Era of the Cloud: An Indian Perspective" (2013) *Law Journal of Higher School of Economics* 3 and Neethling *et al Neethling on Personality Rights* 366.

Act), which is still a Bill at the time of this research. The Act's purpose will be to criminalise cyber activities such as unlawful access, interception and interference of data; unlawful acts in respect of software and hardware tools; cyber fraud, cyber forgery and cyber uttering and malicious communications, which includes a form of "hate speech".[36] A detailed analysis of the Cybercrimes Act falls outside the scope of this research.

Data protection and security comprise one of the legal challenges in cloud computing. Most organisations adopt network-centric and perimeter security, which are generally based on firewalls, intrusion detection systems, and traditional security systems. This type of data and security protection does not provide sufficient protection against cybercriminals, privileged users, or other insidious types of security attacks.[37] A study by the Business Software Alliance South Africa (BSASA) (2012) raised issues relating to software licence abuse and piracy through cloud computing services in the South African context.[38]

The study revealed that about 42% of businesses that use paid cloud computing services around the world were reported to be sharing their log-in credentials within their organisations, while 45% in emerging economies like South Africa with only 30% in mature markets were reported to be sharing their credentials internally.[39] Even though some licences allow sharing accounts, cloud computing service providers do not charge by the seat but by the number of computing resources consumed. About 56% of businesses that use cloud computing services believe that it is wrong to share log-in credentials, which is regarded as software piracy. Other than software piracy, other issues raised included piracy of entertainment, such as music, and infringement of intellectual property rights.[40]

[36] Chapter 2 of the Cybercrimes Act 19 of 2020.
[37] U Yerram "Data Security in the Cloud" (2012) *CSO* http://www.vormetric.com/sites/default/files/wp-data-security-in-the cloud (Accessed 4 May 2020).
[38] A Gillwald, M Moyo and M Altman "Cloud computing in South Africa: Prospects and Challenges" (2012) 58 https://www.researchgate.net/publication/331639595 (Accessed 30 May 2020).
[39] *Ibid*.
[40] *Ibid*.

A close analysis of cloud computing regulation is necessary, as the advent of cloud computing has brought a myriad of legal challenges for protecting the right to privacy.[41] This aspect is a vulnerable part of one's personality rights, especially cloud computing services.[42] Legal protection mechanisms must safeguard the processing of personal information and establish extraterritorial jurisdiction to regulate the use of cloud computing and national legislation.[43] International laws in foreign law, treaties and conventions governing data protection are necessary as cloud computing services have grown to include more users across different countries through their trans-national characteristics.[44]

Moving personal information across multiple jurisdictions creates the need to meet international data protection standards.[45] Legislators in each jurisdiction have attempted to pass laws that protect their constituents. However, jurisdictional issues that threaten the stability of an international cloud computing regime have emerged, hence the need to meet international data protection standards.[46] It seems that cloud computing services have created a dual legal expectation for the legislature to protect the right to privacy nationally and internationally.

Cloud Computing offers users and organisations convenient access to computing without understanding the intricacies of exactly how the processing of personal information is performed within the cloud.[47] To utilise cloud computing requires users and organisations to trust cloud computing service providers with the personal information processed.[48] This subsequently raises issues regarding the security and reliability of the shared pool of computing resources when processing personal information.[49]

---

[41] D C Andrews and J M- Newman "Personal Jurisdiction and Choice of Law in the Cloud" (2013) 73 *Md. L. Rev*. 313 at 315.
[42] S Snail and S Papadopoulos *Cyberlaw @SA III: The Law of Internet in South Africa* 3rd Edition (2012) 277.
[43] Narayanan 2012 *Chicago Journal of International Law* 789.
[44] Narayanan 2012 *Chicago Journal of International Law* 784.
[45] *Ibid.*
[46] Narayanan 2012 *Chicago Journal of International Law* 785.
[47] K Van der Schyff and K Krause "Higher Education and Cloud Computing in South Africa: Towards Understanding Trust and Adoption Issues" (2014) 55 *South African Computer Journal* 40.
[48] *Ibid*.
[49] *Ibid*.

These concerns bring cloud computing under the scrutiny of government regulation on privacy, confidentiality, legal, and contractual concerns, as countries struggle to ensure that their citizens' data is protected. As is common with new technologies, the continuing scientific development of cloud computing is outpacing its legal counterpart for now.[50]

Laws that regulate the processing of personal information have been adopted worldwide since the mid-1970s.[51] For example, in the EU, data protection is an important issue listed as a fundamental right in the Charter of Fundamental Rights (CFR).[52] By the 1980s, data protection had become an international issue.[53]

The emergence of a global market led to an increase in information exchange, including personal information across national boundaries.[54] The flow of information across national borders became the life-blood of the emerging global economy. International organisations such as the Organisation for Economic Co-operation and Development (OECD), the Council of Europe (CE) and the European Community (EC) realised the necessity of harmonising data protection to circumvent the national laws of the country of origin of the data subject on data protection.[55]

1.3.3 The regulatory framework for processing personal information in South Africa

South Africa is one country that has adopted data protection legislation to meet the global data protection standards. Following this global trend, South Africa enacted its privacy legislation, the Protection of Personal Information Act 4 of 2013 (POPI Act). In

---

[50] J R Reidenberg "*Lex Informatica*: The Formulation of Information Policy Rules Through Technology" (1998) 76 *TEX. L. Rev.* 553 at 566.

[51] A Roos "Personal Data Protection in New Zealand: Lessons for South Africa" (2008) 4 *Potchefstroom Electronic Law Journal* 62.

[52] The Charter of Fundamental Rights of the European Union (2000) *Official Journal C* 364/1 provides the following in art 8: Protection of personal data: -
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

[53] A Roos 2007 *SALJ* 403.

[54] *Ibid*.

[55] *Ibid*.

October 2005, the South African Law Reform Commission (SALRC) published a Discussion Paper on privacy and data protection containing a draft Bill on the protection of personal information.[56] The objects of the draft Bill were to give effect to the constitutional right to privacy by safeguarding a person's personal information when processed by public and private bodies. It also aimed to establish mechanisms and procedures in harmony with international prescripts.[57] The SALRC discussion paper introduced the dawn of the POPI Act.

The POPI Act protects the privacy rights determined by section 14 of the South African Constitution that specifies that "everyone has the right to privacy".[58] The right to privacy is a constitutional right enshrined in the Bill of Rights under chapter 2 of the Constitution, subject to limitations aimed at protecting other rights and legally protectable interests.[59] The right to privacy includes the right to protection against unlawful processing of personal information.[60] The POPI Act impacts all who process personal information as part of their business activities.[61] Generally, in South Africa, privacy is recognised and protected as a personality interest in section 14 of the Constitution and the common law.[62]

However, the advancement of technology revealed the inadequacies of the common law protection of data privacy for both natural and juristic persons.[63] Chapter three will provide a detailed discussion and analysis of the constitutional and the common law protection of the right to privacy in the context of cloud computing. As a result, the gap

---

[56] South African Law Reform Commission *Privacy and Data Protection* Project 124 (2005) Discussion Paper 109.
[57] *Ibid*.
[58] Section 14 of the Constitution of the Republic of South Africa 108 of 1996 states that;
Everyone has the right to privacy, which includes the right not to have-
(a) their person or home searched;
(b) their property searched;
(c) their possessions seized; or
(d) the privacy of their communications infringed.
[59] Section 14 of the Constitution.
[60] The Preamble of the Protection of Personal Information Act 4 of 2013.
[61] M de Bruyn "The Protection of Personal Information (POPI) Act - Impact On South Africa" (2014) 13(6) *International Business and Economics Research Journal* 1325 and Neethling *et al Neethling on Personality Rights* 366.
[62] K Feng and S Papadopoulos "Student (K-12) Data Protection in the Digital Age: A Comparative Study" (2018) 51 *Comparative and International Law Journal of Southern Africa* 261 at 269.
[63] J Neethling *et al Neethling's Law of Personality* 2nd Edition (2005) 267.

in the common law necessitated the need to promulgate the POPI Act to deal with the protection of personal information.[64] The preamble of the POPI Act further recognises that the state must respect, protect, promote and fulfil the rights contained in the Bill of Rights.[65] Chapter four of the study will analyse the selected provisions of the POPI Act on the regulation of privacy in a cloud computing context.

1.4 The research questions

The research questions are stated as follows:

1. Do the South African Constitution and the common law adequately protect the right to privacy in the context of cloud computing services?
2. Does the POPI Act provide "adequate" data protection standards and fill all the gaps identified under the common law and the constitutional data protection remedies?
3. Does the POPI Act meet the international data protection standards set by the General Data Protection Regulation (GDPR) on international data breaches in the context of cloud computing?
4. Are there possible recommendations and suggestions that would assist in improving South Africa's legal framework on data protection to meet international data protection standards?

1.5 Goals of the research

The research aims to analyse and determine whether the POPI Act can offer adequate data protection in the form of remedies and enforcement mechanisms for international data breaches in cloud computing services. The objectives of the research are:

a) To reveal the shortcomings under the South African Constitution and the common law that led to adopting the POPI Act by analysing the regulation of cloud computing services.
b) To determine the shortcomings of the POPI Act in the context of cloud computing.

[64] Feng 2018 *CILSA* 269.
[65] *Ibid*.

c) To determine the application of the GDPR on international data breaches and compare its provisions with the POPI Act in the context of cloud computing.
d) To make recommendations after determining the application of both legislations in the context of cloud computing and international data privacy violations.

1.6 Methodology

This is a desktop-based research study. The research will make use of the published reports and statistics. In the context of this study, this will include all sources of information that do not involve a field survey. The research will use primary sources and secondary sources, for example, the Constitution, legislation, case law, textbooks, journals, articles, and other international agreements and conventions. This entails collecting and analysing relevant material from the indicated sources to arrive at a deeper understanding of the use of cloud computing as a mechanism to process personal information.

The interpretation of statutes approach will also be employed in this study. Different theories of statutory interpretation will be used on the POPI Act's regulation of the right to privacy and the protection of personal information in the context of cloud computing in Chapter 4 of the study. These theories will determine whether the POPI Act's remedies, including civil remedies under section 99, provide adequate international data protection standards and under what circumstances.

The study also entails a comparative analysis. This will provide a foreign law model (GDPR) to improve a domestic law model (POPI Act). The analysis will promote the international unification and harmonisation of law as far as data protection is concerned in the context of cloud computing.[66] The comparative analysis focuses on the fact that, despite the apparent importance of data protection law standards worldwide, the POPI Act might be considered an intermediary to ensuring compliance

[66] M Reimann "The End of Comparative Law as an Autonomous Subject" (1996) 11 *Tulane European and Civil Law Forum* 49 at 54.

to the GDPR as one of the most influential pieces of legislation on cross-border flow of personal information.[67]

The comparative approach will assist in determining, evaluating, and testing the extent and scope of the GDPR and its remedies on data breaches that occur on cloud computing services. It will further determine if the POPI Act is still aligned with the most recent international data protection instruments.

As the research is based on publicly available documentary data, no ethical considerations apply.

1.7 Limitations of the study

The first limitation relates to the highly technical nature of the topic as the research centres on the regulation of cloud computing and information technology space. The growth of technology and innovation is highly controversial and brings the perennial debate on the relationship between law and technology. The extent to which cloud computing affects the adoption of data protection laws and, more specifically, the pace at which technology keeps evolving have become a source of controversial debate.

Since the researcher has no solid background and technical training in IT, the discussion in this thesis is restricted as much as possible to legal challenges in the context of cloud computing. As a result, some of the issues which may affect the outcomes analysed in the thesis, such as the technical controls adopted and put in place by cloud computing service providers to mitigate data breaches such as firewalls and data encryption methods, fall beyond the scope of this thesis. This makes the thesis have a narrower perspective than is necessary to fully comprehend and resolve the relationship between law and IT in the context of cloud computing.

The second limitation relates to the fluid and diverse nature of the topic. In this research, so many developments could occur on issues directly relevant to the topic

[67] C Yav "Perspectives on the GDPR from South Africa" (2018) 2 *International Journal Data Protection Officer, Privacy Officer and Privacy Counsel* 19.

of discussion. For example, certain parts of the POPI Act are not yet in force since its partial commencement in 2014[68] and 2020[69] The proclamation affects the POPI Act's remaining provisions and the regulations that might have changed in due courses, such as the 2018 regulation relating to the POPI Act.[70] Should there be any changes pertaining to the full commencement of the POPI Act and the regulations, this could affect the research in providing a comprehensive and persuasive conclusion and recommendations of the study.

Furthermore, IT is a forever growing and evolving industry; new technological advancements are introduced regularly, affecting the current features and characteristics of cloud computing services. These two issues demonstrate the ever-changing and developing nature of the topic of discussion.

The above-highlighted factors can affect the research in two ways. First, due to the ever-growing number of issues to consider, it is impossible to explore all the relevant ones in sufficient depth within the time allocated for the research. Secondly, due to the novelty of some of the issues under discussion, it could be challenging to find academic writing and other reliable material to aid with the research.

The information available concerning some relevant issues is mainly in articles, especially in the second chapter of the research under cloud computing regulation and contextualisation. Some sources are not subject to peer review and therefore cannot be relied on to substantiate research claims. The inability to explore issues in detail and the limited material available on certain sections of the study may hinder the researcher from fully understanding the research topic.

The research study aims to determine whether the POPI Act provides "adequate" data protection. The discussion will focus on some of the provisions that are considered essential to attaining adequacy that meets international data protection standards. In

[68] Protection of Personal Information Act Proclamation, GN R25, *Government Gazette* 37544, 11 April 2014.
[69] Protection of Personal Information Act Proclamation, GN R21, *Government Gazette* 43461, 22 June 2020.
[70] Protection of Personal Information Act Regulations, GN R1383, *Government Gazette* 42110, 14 December 2018.

this sense, the discussions rely on the guidance provided by the GDPR on the meaning of “adequate” data protection. Therefore, the conditions for the lawful processing of personal information and other provisions of both legislations selected for comparison will not be discussed extensively in this study. The time allocated for completing this research is minimal to cover a comprehensive analysis of all the conditions in the context of cloud computing. The research also seeks to address all industries that process personal information as part of their daily operational requirements, governments and the data subjects to whom the personal information relate.

1.8 Structure and overview of the thesis

Chapter One: Introduction

The current chapter introduces the thesis. It discusses the background and context of the research, states the main problem tackled by the thesis, highlights the research questions, explains the research methodology and outlines the goals of the research.

Chapter Two: Cloud computing as a mechanism to process personal information

The second chapter deals with the regulation of cloud computing as a mechanism to process personal information. The focus is on the regulation of cloud computing services and the jurisdiction of data protection authorities to regulate cloud computing. The chapter also focuses on the jurisdictional reach of data protection laws adopted by different jurisdictions to regulate cloud computing.

Chapter Three: The right to privacy under the common law and the Constitution in the cloud computing context

The third chapter focuses on the critical analysis of the right to privacy and its recognition under section 14 of the South African Constitution and the common law.

Chapter Four: The influence of the Protection of Personal Information Act 4 of 2013 (POPI Act) on the regulation of privacy in the Cloud Computing context

The fourth chapter deals with the influence of the POPI Act on privacy regulation in a cloud computing context. The chapter will also analyse the remedies and enforcement mechanisms of the POPI Act in the context of cloud computing.

Chapter Five: A comparative study of the Protection of Personal Information Act 4 of 2013 (POPI Act) and the General Data Protection Regulation (GDPR)

Chapter five is a comparative study of the POPI Act and the GDPR: The Scope of the GDPR, similarities and differences of the POPI Act and the GDPR, enforcement of the GDPR on cloud computing services and the remedies of GDPR on cloud computing data breaches will be analysed.

Chapter six: Recommendations and conclusion

This chapter ties together the findings from the above chapters and contains the thesis summary, recommendations, and conclusion.

1.9 Conclusion

As much as South Africa has adopted the data protection legislation, data protection regulation remains vital to ensure the strict guidelines and enforceability of the POPI Act. Cloud computing is a new fact and phenomenon in the entire international law corridor. International law such as conventions, treaties and foreign law legal response places cloud computing data breaches as a new kind of international crime that has not been regulated fully both domestically and internationally.[71] The need for the proper regulation of cloud computing and data protection, in general, is highly urgent to be created to mitigate data breaches. It is considered that the regulation should be governed by international law product universally.[72] The universal nature will provide data breaches with legal status in international law, and this will further assist in the adoption of domestic data protection laws to be aligned with the international data protection standards

[71] M A Manuputty, S M Noor and J Sumardi "Legal's Standing of Cyber-Crime in International Law Contemporary" (2014) 22 *Journal of Law, Policy and Globalization* 128 at 132.
[72] *Ibid.*

Chapter 2: Cloud computing as a mechanism to process personal information

2.1 Introduction

In recent history in the IT space, there has been a prevalence of reports on data breaches within various organisations worldwide. A study conducted in the United States of America (USA), investigating 529 data security breach cases, found 1.9 billion compromised records. The majority of those compromised records were within corporations.[73] Although one would think that only small and large corporates would suffer this fate, more and more governments, universities and healthcare providers have become prime targets of data breaches.[74] These data breaches call for more robust legal protection instruments for data subjects who usually become victims.

This chapter focuses on the regulation of cloud computing as a mechanism to process personal information and the jurisdiction of data protection authorities to regulate cloud computing.

The chapter will analyse the international law implications of cloud computing by identifying two equilibria of a global cloud computing system. The first state is where countries use jurisdictional theories and principles to provide extraterritorial data protection laws. The second state is one in which countries cooperate through an international agreement or organization to find a common solution to the risk of data breaches in cloud computing,[75] for example, General Agreement on Trade in Services, Marrakesh Agreement Establishing the World Trade Organisation.[76] The last section will provide the concluding remarks of the chapter.

[73] N Baloyi and P Kotze "Are Organisations in South Africa Ready to Comply with Personal Data Protection or Privacy Legislation and Regulations?" (2017) *International Information Management Corporation* 1 http://www.ist-africa.org /Conference2017 (Accessed 31 May 2020).

[74] Olorunju 2019 *Journal of Public Administration* 363.

[75] Narayanan 2012 *Chicago Journal of International Law* 789.

[76] General Agreement on Trade in Services, Marrakesh Agreement Establishing the World Trade Organization (1994) 1869 UN Treaty Ser 183 (GATS) and M V P Asinari "The WTO and the Protection of Personal Data. Do EU Measures Fall Within GATS Exception? Which Future for Data Protection within the IVTO E-Commerce Context?" (2003) 18th *BILETA Conference* http://www.bileta.ac.uk/Document%20Library/1/ pdf (Accessed 04 July 2020).

2.2 Contextualization of cloud computing

Before a substantive discussion of applicable law and jurisdiction, it may be apt to contextualise cloud computing. Apart from the base definition of cloud computing services as discussed in the previous chapter, there are five essential characteristics mentioned in the definition, which requires some consideration and a brief discussion. These are: (a) on-demand self-service, (b) broad network access, (c) resource pooling and location independence, (d) rapid elasticity and (e) measured services.[77]

Firstly, the on-demand self-service feature empowers the end-user to control and manage IT resource provisioning directly. The service provides access to different cloud computing services when the end-users require them. [78] The second characteristic is the broad network access that allows the end-user to manage and control their cloud computing environment through broad network access or a web browser, irrespective of their location. Typically, access can be gained through any automated or electrical gadget such as personal computers, laptops, smartphones, or other devices.[79] The service becomes location independent and enables the cloud computing services users to work "over the cloud computing".[80]

The third characteristic is resource pooling and location independence. This function is an essential aspect of the cloud computing platform environment. It caters for efficient resource sharing among multiple users and customers from around the world in different data centres. It is more commonly referred to as multi-tenancy in larger cloud computing systems. This is where users can share costs and resources within a single system, making cloud computing systems more cost-effective.[81]

The fourth support aspect, rapid elasticity, works in areas where the hardware resources are expected to be shared and provisioned in real-time when required. The end-user can seamlessly utilise resources on demand and not have any part of the

[77] Mell "The NIST Definition of Cloud Computing" 2.
[78] Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 24.
[79] *Ibid.*
[80] *Ibid.*
[81] J Sluijd, P Larouche and W Sauter "Cloud Computing in the EU Interoperability, Vertical Integration and the Internal Market" (2012) *Tilburg Law and Economics Centre (TILEC)* 14 https://www.jipitec.eu/ (Accessed 04 April 2020).

services affected. Cloud computing systems have been designed to function with elasticity, scalability and customisation to meet such needs and demands, making resources appear to be virtually unlimited.[82]

In the cloud environment, choices and options for users can be built into software platforms, whereas the cloud computing service providers can profit from the 'economies of scale.' The fifth and last essential characteristic is measured services. It means that any cloud systems element, such as computation power, storage medium, and IT devise, can be converted into a measurable charging plan or structure.[83] Cloud computing service providers then have control over both the storage and infrastructure. Depending on the delivery model and Service Level Agreement (SLAs) set up with end-users, the end-users will have to pay for the services according to the service charge plan.[84]

In the value chain of the cloud computing model, data is initially processed by the outsourcing business, for example, an employer; after that, it gets transmitted to the service provider such as iCloud. It is then processed by the service provider, stored within the service provider's computers, and then remotely accessed through a network.[85] In some cases, the data is partially and periodically downloaded to local servers at the outsourcing business for local viewing or customised reporting.[86] For example, Amazon Web Services, one of the leaders in cloud computing, now offers data storage, data processing and database management services through the Internet.[87] While cloud computing is often talked of as something taking place in the distant obscure, in reality, it must ultimately use physical computers, with physical storage facilities housed in physical structures.

---

[82] Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 25.
[83] *Ibid.*
[84] *Ibid.*
[85] J N Hoover and R Martin "Demystifying the Cloud" (23 June 2008) *INFO WK* 32 http://www.informationweek.com/news/services/hostedapps/showArticle.jhtml?articleID=20870073 (Accessed 04 April 2020) (Noting that common characteristics of cloud computing include "IT resources provisioned outside of the corporate data centre, those resources accessed over the Internet, and variable cost attached to them".).
[86] Hoover and R Martin "Demystifying the Cloud" and Dixon 2012 *Judges Journal* 36.
[87] *Ibid.*

2.3 Types of cloud computing services

The cloud computing services may be deployed in either of the two ways, and that is, privately within an organisation in which it has been set up and publicly.[88] The public cloud computing model will be discussed in detail in this section of the study. Private cloud computing services have fewer risks and difficulties than public cloud computing services.[89] An indication of some of the primary risk and challenge areas inherent in the public cloud include personal data protection, digital operational management, increased security vulnerability and cross-border movement, together with data portability of IT resources.[90]

The public cloud computing model is open and divided into three main segments: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).[91] These cloud computing services form a spectrum, from low-level (IaaS) to high-level (SaaS) functionality, with PaaS in between.[92]

The lower level is the IaaS, which provides essential computing functions such as data storage, processing power and communications.[93] IaaS requires user sophistication and expertise and affords the user flexibility and control.[94] IaaS services, such as Amazon's Elastic Computer Cloud (ECC),[95] offer flexibility and scalability by furnishing customers with access to virtual servers to install and maintain their software.[96]

PaaS refers to a cloud platform, which offers an environment where developers create and host web applications.[97] Google App Engine is an example of a PaaS. It allows

[88] Information Systems Audit and Control Association "IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud" (2011) *ISACA* http://www.isaca.org/ (Accessed 05 July 2020).
[89] Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 19.
[90] *Ibid.*
[91] V Shetty "Computing the Tax on Cloud Computing" (2014) 8 *Law Review Government Law College* 159 at 160, Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 19 and ISACA "IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud".
[92] Narayanan 2012 *Chicago Journal of International Law* 786 and Mell "The NIST Definition of Cloud Computing" 2 and W K Hon, J Hörnle and C Millard "Data Protection Jurisdiction and Cloud Computing: When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing" (2012) 26 (2-3) *International Review of Law, Computers and Technology* 129 at 130.
[93] Dixon 2012 *Judges Journal* 36.
[94] Mell "The NIST Definition of Cloud Computing" 2 to 3.
[95] Amazon EC2 Amazon web services 2 http://aws.amazon.com / (Accessed 04 July 2020).
[96] Mell "The NIST Definition of Cloud Computing" 3.
[97] *Ibid.*

programmers to create and customise software applications. A PaaS customer does not need to manage processing or storage services actively; they can just focus on programming applications.[98] PaaS options such as the Google App Engine have aspects of both preceding branches in that they use an entire platform hosted on the provider's server. Often these include everything from an operating system to developer tools.[99]

SaaS is the top layer of the cloud.[100] It refers to end-user applications or software used or accessed via the Internet.[101] SaaS requires little technical know-how on users and is the most commonly used among consumers.[102] Common SaaS applications include e-mail, backup or disaster recovery, storage, and web hosting services.[103] It provides users with fully functioning applications that rest entirely on the cloud. SaaS providers install and run software on their servers, which customers access remotely.[104]

The most common SaaS services are Salesforce.com's online management tools,[105]Google Docs, Google Spreadsheets, and the Chrome OS.[106] Google Docs is an online storage and software service that offers a word processor, spreadsheet editor, and presentation editor that allows creating, storing, and sharing documents and collaborating with others.[107] Google also offers other services such as calendar and e-mail (Gmail).[108]

---

[98] Mell "The NIST Definition of Cloud Computing" 4 to 5.
[99] Mell "The NIST Definition of Cloud Computing" 2 to 3.
[100] R Berry and M Reisman "Policy Challenges of Cross-Border Cloud Computing" (2012) *Journal of International Commerce and Economics:* United States International Trade Commission 2 https://www.usitc.gov /journals/policy-challenges of cross-border cloud computing pdf (Accessed 06 July 2020).
[101] *Ibid.*
[102] *Ibid.*
[103] W K Hon and C Millard "Cloud Technologies and Services" (2013) *Cloud Computing Law Oxford: Oxford University Press* 3 at 5.
[104] Mell "The NIST Definition of Cloud Computing" 2.
[105] A Monaco "A View Inside the Cloud*"* (7 June 2012) *The Institute IEEE Spectrum* http://theinstitute.ieee.org/technology-focus/technology-topica-viewinside-the-cloud (Accessed 03 July 2020).
[106] *Ibid*.
[107] *Ibid.*
[108] Dixon 2012 *Judges Journal* 36.

One cloud computing service may involve different layers of service providers, not always to the customer's knowledge, and perspective effects classification. For example, customers of storage service DropBox may consider it a SaaS, while for DropBox, which uses Amazon's IaaS infrastructure to provide its service, Amazon provides IaaS. A Dropbox is a cloud storage service that allows users to store, share, and automatically synchronise files between different devices.[109] Dropbox offers a free account with 2 Gigabytes (GB) of storage, which one may upgrade to a monthly subscription account that grants the user a higher storage limit.[110]

Also, PaaS may be layered on IaaS, and SaaS may be layered on PaaS or IaaS.[111] For example, PaaS service Heroku is based on Amazon's Elastic Compute Cloud (EC2) IaaS.[112] Amazon Cloud Drive (ACD) is a cloud storage service. It gives 5 GB of storage space for free and can be upgraded with a yearly subscription service.[113] Amazon is one of the largest public cloud computing service providers and one of the least expensive cloud storage services.[114] The maximum file size permitted is 2 GB, whether the user has a free or subscription account. Amazon Cloud Drive does not, however, offer a file-sharing feature.[115]

Cloud computing can also be classified into four deployment models based on the nature of the network. These four deployment models are:

Private cloud: This is a cloud computing infrastructure owned or leased for exclusive use by a single organisation comprising multiple consumers.[116] This type of deployment model is predominantly found in office units and classrooms.[117]

---

[109] *Ibid*.
[110] *Ibid.*
[111] Mell "The NIST Definition of Cloud Computing" 2 and Hon 2012 *International Review of Law, Computers and Technology* 130.
[112] *Ibid.*
[113] Hon 2012 *International Review of Law, Computers and Technology* 130.
[114] Dixon 2012 *Judges Journal* 36.
[115] *Ibid.*
[116] Mell "The NIST Definition of Cloud Computing" 3 and Shetty 2014 *Law Review Government Law College* 160.
[117] Hon 2012 *International Review of Law, Computers and Technology* 130.

Community cloud: This is another form of cloud computing infrastructure. It is shared amongst several organisations from a specific community with a common concern, such as multinational corporations. Community clouds are generally designed for specialised and highly regulated industries, such as healthcare or investment banking.[118] A community cloud would be built to handle that specific industry's security and regulatory compliance requirements.[119] Some public organisations using these services are South African government users or local government bodies.

Public cloud: Public cloud computing offers solutions, applications and storage to almost anyone who has access to the internet. This is done so that different users may be serviced using the same hardware or application software and stored in the same database.[120] Public cloud services may be free or offered on the pay-perusage model.[121] Examples of public cloud include SalesForce.com, Google App Engine and Amazon EC2.[122]

Hybrid cloud: This is another form of cloud computing infrastructure. It is a composition of two or more clouds such as private, community or public cloud. They, however, remain as unique entities but are bound together, enabling data and application portability.[123] An example of a hybrid cloud is cloud bursting.[124] In cloud bursting, organisations use their private computing infrastructure for normal usage but access the services on a public cloud using services for high load requirements.[125] This ensures the handling of a sudden increase in computing requirements and load balancing between clouds.[126]

---

[118] Techopedia "Techopedia Explains Community Cloud" (2 May 2020) http://www.techopedia.com /definition/community cloud (Accessed 13 July 2020).
[119] *Ibid.*
[120] Hon 2012 *International Review of Law, Computers and Technology* 130.
[121] *Ibid* and Hon 2013 *Cloud Computing Law Oxford: Oxford University Press* 5.
[122] R Buyya *et al Mastering Cloud Computing: Foundations and Applications Programming* (2013) 25.
[123] J Ryan "The Uncertain Future: Privacy and Security in Cloud Computing" (2014) 54(2) *Santa Clara Law Review* 497 at 503 and Hon 2012 *International Review of Law, Computers and Technology* 130.
[124] *Ibid.*
[125] *Ibid.*
[126] S R Smoot and N K Tan *Private Cloud Computing: Consolidation, Virtualization, and Service-Oriented Infrastructure* (2011) 9.

The reference model for cloud architecture defines five major players in delivering cloud computing services. These are the cloud consumer, cloud service provider, cloud carrier, cloud auditor and the cloud broker. Each of these named players is an entity, person or organisation that participates in a transaction or process and performs tasks within the cloud computing platform.[127]

The rapid development of computer connectivity, the role and the introduction of cloud computing have compelled national governments and international agencies to address the need for regulation and safety of personal information.[128] Policymakers and industry leaders echo further concerns,[129] furthering the 'legal debate' on the risks and challenges within cloud computing databases.[130] While computers themselves do not commit crimes, they and the Internet have created a new generation of crimes. Human intervention ignites criminal activity while the automated machines carry on the major activities.[131] These computer crimes, also known as cybercrime, use computers as instruments to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.[132]

In principle, cloud computing data breaches can be perpetrated from anywhere and against any data subject in the world. Effective investigation and prosecution of such data breaches often require tracing criminal activity through several national borders.[133] Several cloud computing service providers and users are spread over different jurisdictions may also be involved in an investigation. Often, perpetrators of data breaches in cloud computing exploit the transnational characteristics of the

[127] Smith "Cloud Computing for Business and Society" and Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 18 to 19.
[128] R Broadhurst "Developments in the Global Law Enforcement of Cyber-Crime" (2006) 29 *An International Journal of Police Strategies and Management* 408 and Smith "Cloud Computing for Business and Society".
[129] Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 19 and Smith "Cloud Computing for Business and Society".
[130] Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 19.
[131] F Talat "Cyber Crimes: Challenging the Paradigms of Traditional Criminal Law" (2005) 3 *Corporate Law Cases* 475 and M Singh and S Singh "Cyber Crime Convention and Trans-Border Criminality" (2007) 1 *Masaryk University Journal of Law and Technology* 53.
[132] M A Dennis "Cybercrime Law" *Britannica* https://www.britannica.com/topic/cybercrime (Accessed 23 February 2022).
[133] Singh 2007 *Masaryk University Journal of Law and Technology* 54.

information infrastructure. The perpetrators avoid prosecution by complicating investigations.[134] They are presumed to initiate data breaches from countries with inadequate data protection laws; personal Information gets routed through countries with different laws and practices and no structures for cooperation.[135]

2.4 The introduction of cloud computing in the IT space

John McCarthy, the man who introduced the phrase "Artificial Intelligence" (AI).[136] He predicted that computing power would become a public utility, a service directly provided or heavily regulated by the governments.[137] This prediction was based on the observation of the speed at which IT was taking over the traditional way of processing personal information. In the past decades, personal information processing using computers has become ubiquitous.[138] As mentioned above, today, IT is exploring a new frontier in the processing of personal information,[139] which is the use of cloud computing.[140]

The use of cloud computing has become the enticing alternative to "do-it-yourself" in IT solutions. It provides shared public access to a modern need. Owing to the general operational structure of cloud computing, it is subject to increasing regulation, coming close to fulfilling McCarthy's prediction.[141]

Both individuals and businesses have embraced cloud computing as the future of IT. The study conducted by The Economist revealed that, as early as 2008, about 69% of the American population connected to the web using cloud computing services, such

[134] S D Abraham *et al* "A Proposal for an International Convention on Cyber Crime and Terrorism" (2002) *The National Academic Press* http://www.iwar.org.uk/law/ resources/cybercrime/stanford/cisac-draft.htm (Accessed 01 July 2020).
[135] *Ibid*.
[136] E Dou "Is Europe Ready to Put Its Data in the Clouds?" (27 April 2011) *AI Brand Channel=O* 1 http://af.reuters.com/article/ethiopiaNews/ idAFLDE7341NU20110426 (Accessed 04 April 2020).
[137] *Ibid.*
[138] Van der Merwe *et al ICT Law* 364.
[139] Carpenter Jr 2010 *Washington Journal of Law Technology and Arts* 2.
[140] Peihani 2017 *Singapore Journal of Legal Studies* 79.
[141] Narayanan 2012 *Chicago Journal of International Law* 784, A C Krikos "Cloud Computing as a Disruptive Technology" (2011) 2 http://www.media.cloudbook.net /pdf/ (Accessed 03 July 2020) and Peihani 2017 *Singapore Journal of Legal Studies* 77.

as e-mail or online data storage services.[142] Companies, too, have moved to cloud computing services.[143]

The transition to use cloud computing services allows companies to process massive amounts of data and tailor their services to the needs of consumers efficiently.[144] For instance, AccuWeather, which provides weather forecasting to approximately 175,000 clients with a viewership of more than 1 billion, uses a cloud computing services infrastructure.[145] This infrastructure allows it to handle 10 billion data requests every day while reducing IT costs by 40%. [146] Airbnb, which lets travellers book accommodation from guest hosts, also uses cloud computing services infrastructure.[147] This firm has managed to create a supply of accommodation that allows suppliers and renters to share feedback, images, and reviews all through the cloud computing platforms.[148]

SunTrust Bank, a US bank with total assets estimated at $178.2 billion, has transitioned from loan origination and underwriting to cloud computing platforms.[149] The move eliminates complex back-end systems and difficulties in getting timely access to customer information.[150]

The introduction of cloud computing platforms has created complex legal and regulatory challenges. The growing concern on the legalities associated with cloud computing services explores issues posed by the cloud computing services. These

---

[142] M Peihan "Let It Rise: A Special Report on Corporate IT" (2008) *The Economist* 3 http://the.economist.com /node/12411882 (Accessed 03 July 2020).
[143] *Ibid.*
[144] *Ibid.*
[145] C Cooper "The Cloud Drives a New Wave of Disruption" (25 June 2015) *CIO* http://www.cio.com/article/2940519/cloud-infrastructure/the-cloud-drives-a-new-wave-of-disruption.html (Accessed 03 July 2020).
[146] *Ibid*.
[147] *Ibid.*
[148] Amazon Web Services "Airbnb Case Study" https://www.amazon.com / solutions/case-studies/airbnb/ (Accessed 03 July 2020).
[149] SunTrust Banks "Improving Productivity, Reducing Vulnerability Windows" (25 February 2011) *International Business Machines Corp (IBM*) http://www-03.ibm.com /software/ business case studies/us/en/corp?synkey=Y818919Pl8846W63 (Accessed 04 July 2020) and E McCormick "Is Banking's Future in the Cloud?" (12 September 2012) *BankDirector.com* http://www.bankdirector.com/ (Accessed 04 July 2020).
[150] *Ibid*.

include concerns such as confidentiality and privacy and its relationship to the law, such as in contract formation and securing intellectual property.[151] One area that has not yet received much attention is how cloud computing technology impacts the regulators as far as data protection regulation is concerned.[152]

2.5 Concerns over continuous cross border free flow of personal information

Cloud computing services for processing personal information demand a highly flexible computing environment and seek to achieve more predictable costs.[153] However, the use of cloud computing to process personal information has created privacy concerns for both data subjects and the responsible parties.[154] Data breaches in cloud computing are a new range of national law and international criminal law.[155] The international community should take these crimes seriously; an immediate response form is needed to regulate cloud computing. This must be done internationally because so far, few conventions have found cybercrime internationally, such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) EX.CL/846(XXV) 2014 and the Convention on Cyber Crime of the Council of Europe (Budapest Convention) ETS No. 185, 2001.[156] One of the risks of using cloud computing is the confusion about applicable laws, the changing regulatory climate, and the lack of industry standards.[157]

The first concern of cloud computing services relates to the continuous cross-border free flow of personal information for commercial purposes through cloud computing

[151] Ryan 2014 *Santa Clara Law Review* 497, J A Stiven "Preparing and Advising Your Clients on Cloud Usage" (2014) 12 (4) *DePaul Bus and Commercial Law Journal* 421, F Pasquale and T A Ragone "Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing" (2014) 17 *Stanford and Technology Law Review* 595, C Reed "Information Ownership in the Cloud"(2009) Queen Mary University of London, School of Law, Legal Studies Research Paper No 45/2010, W K Hon C Millard and I Walden "Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now" (2012) 16 (1) *Stanford and Technology Law Review* 79, T N Foster "Navigating Through the Fog of Cloud Computing Contracts" (2013) 30(1) *The John Marshall Journal of Information Technology and Privacy Law* 13 and F Tasneem "Electronic Contracts and Cloud Computing" (2014) 9(2) *Journal of International Commercial Law and Technology* 105.

[152] *Ibid*.

[153] Carpenter 2010 *Washington Journal of Law Technology and Arts* 1.

[154] Solms 2012 *Journal of Business Management* 77.

[155] Manuputty 2014 *Journal of Law Policy and Globalization* 128.

[156] *Ibid.*

[157] *Ibid.*

platforms.[158] Cloud computing services assist in increasing efficiency and reducing infrastructure costs in commercial activities.[159] However, they pose challenges for many governments as interoperability issues arise.[160] Furthermore, there could be duplication of certain personal information processed offline through the use of cloud computing services.[161]

The second concern is its portability because its model requires that data reside with the service provider. Because of the operational configurations of the cloud computing mechanism, the cloud computing service providers generally operate against international law, particularly data protection law and privacy regulations.[162] As users of cloud computing services process data on the cloud, they are exposed to the risk of data loss and violations of privacy.[163] Generally, once the information has been processed in the cloud, cloud computing service providers bear the burden to minimise the risks of data breaches.[164]

The third concern is the dual criminality for data breaches in the context of cloud computing.[165] For the dual criminality concept, location independence is a crucial characteristic of cloud computing.[166] Therefore, It is often not evident for criminal justice authorities in which jurisdiction the data is stored or which legal framework applies to data protection.[167] A service provider may have its headquarters in one jurisdiction and apply the legal framework of a second jurisdiction while the data is stored in a third jurisdiction.[168] Data may be mirrored in several or move between jurisdictions. If data location determines the jurisdiction, it is conceivable that a cloud

[158] P S Mvelase *et al* "Towards a Government Public Cloud Model. The Case of South Africa" (3-5 June 2013) *Cluster Computing Conference Paper* 149 http://hpc-ua.org/cc-13/files/proceedings/33.pdf (Accessed 7 July 2020).
[159] *Ibid.*
[160] *Ibid.*
[161] Hon 2011 *IDPL* 211.
[162] Narayanan 2012 *Chicago Journal of International Law* 787.
[163] Van der Merwe *et al ICT Law* 367.
[164] *Ibid.*
[165] S L Howard "The Web That Binds Us All: The Future of Legal Environment of the Internet" (1997) 19 *Houston Journal of International Law* 501.
[166] T-CY Cloud Evidence Group Crime Convention Committee "Criminal Justice Access to Data in the Cloud: Challenges" (26 May 2015) Discussion Paper Strasbourg; France https://rm.coe.int/1680304b59 (Accessed 23 February 2022).
[167] *Ibid*.
[168] *Ibid.*

computing service provider systematically moves data within the cloud to prevent criminal justice access.[169]

This concept of dual criminality implies that extradition will not be granted unless an act of the data breach through cloud computing platforms constitutes a crime under the laws of both states.[170] This applies to both the state requesting extradition and the state from which extradition is requested.[171] This can often be a loophole in the system when the perpetrator's country does not have specific legislation concerning data breaches, but the victim's country does.[172] In such situations, applying a nation's domestic laws usually fails to provide effective extra-territorial remedial enforcement mechanisms.[173]

The intangible nature of computer evidence poses another challenge to investigating data breaches.[174] Paper, which is presumed as one of the reliable sources of evidence, has a limited role in cloud computing data breach investigations.[175] Firstly, the intangible and transient nature of data and the technical nature of evidence and investigation on cloud computing data breaches might give the defence claims of technical error, thereby making the prosecution's case weak.[176] Investigation proceedings could further suffer a setback due to the ability to destroy, alter data on the system or move it around within the cloud, thus creating difficulties in obtaining valuable evidence.[177]

Furthermore, conducting investigation measures such as search, seizure and confiscating the computer machinery has certain difficulties. The human rights violations and the right to privacy could be raised as a concern to prevent or delay the process of search and seizures.

---

[169] *Ibid*.
[170] Singh 2007 *Masaryk University Journal of Law and Technology* 56.
[171] *Ibid.*
[172] Howard 1997 *Houston Journal of International Law* 501.
[173] *Ibid.*
[174] Talat 2005 *Corporate Law Cases* 478.
[175] *Ibid.*
[176] *Ibid* and Singh 2007 *Masaryk University Journal of Law and Technology* 56.
[177] S L Hoppkins "Cyber Crime Convention: A Positive Beginning to a Long Road Ahead" (2003) 2 *Journal of High Technology Law* 102.

Secondly, the presence of specially trained and skilled personnel able to duly conduct these actions is required. Thirdly, upon the confiscation of computer machinery containing vital information for an investigation, the possibility of its modification and termination should be looked into and subsequently excluded.[178] However, as mentioned above, although falling out of the scope of this research, the Cybercrimes Act, which is still a Bill at the time of this study, will add immense value to regulate some of these highlighted issues. It can be argued that the Act will provide legal remedies to the affected parties, but the technical complexities of securing computer evidence will remain a challenge. The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), which is also not in force yet, would add value to deal with cybercrimes on a regional level.

These actions should be conducted within a minimum period, considering the speed of receiving the information. Fourthly, careful analysis of the computer system records should be made before confiscating the computer system.[179] This is necessary for the entire procedure of conducting the measures on arrest and seizure of evidence.[180]

With the introduction of cloud computing, it has been suggested that even the development of international law in this area is currently ineffective to control or regulating the cross-border flow of personal information.[181] To be held responsible under principles of international law such as the subjective and objective territorial principles discussed below, the perpetrator must commit a defined offence under customary international principles, as established by international treaties or norms.[182] Due to the relative novelty of data breaches in cloud computing, no or very few international norms presently exist.[183]

[178] Singh 2007 *Masaryk University Journal of Law and Technology* 57.
[179] *Ibid.*
[180] G Vladimir "International Cooperation in Fighting Cyber Crime" (2005) *Computer Crime Research Center* http://www.crime-research.org /articles/Golubev045/ (Accessed 02 July 2020).
[181] G E Coffield **"**Love Hurts: How to Stop the Next 'Love Bug' From Taking a Bite Out of Commerce" (2001) 20 *Journal of Law and Commerce* 254.
[182] Coffield 2001 *Journal of Law and Commerce* 254.
[183] Singh 2007 *Masaryk University Journal of Law and Technology* 57.

The Internet is not a single entity; no government, company, or individual owns it; therefore, the information processed in the cloud knows no boundaries.[184] The transnational characteristic of cloud computing functioning makes jurisdictional issues an important area of concern. The service providers and cloud computing users are usually domiciled in multiple geographical jurisdictions. However, it is imperative that regional and international agreements on jurisdiction and remedial enforcement mechanisms be vigorously enforced. International cooperation is imperative for any fight against data breach controls to be effective.

2.6 Which law applies to the data in the cloud?

In the global development of data privacy protection, Bennett and Raab presented their main research question as to whether there was what they termed "a race to the bottom, race to the top or something else" in what is still the most systematic global review of data privacy regulation.[185] They correctly cautioned that a data privacy law's existence and formal strength is only one factor by which one can measure data privacy protection in a country. Two other dimensions are the effectiveness of enforcement mechanisms and the extent of surveillance. Therefore, there is more than one race to the top or bottom globally. They noted that, concerning legislation, the main conditions proposed by globalisation theories of regulation for a race to the bottom, data mobility and wide national divergence laws were present in the case of data protection legislation.[186]

The cross-border flow of personal information on cloud computing creates challenges for regulators, lawmakers, and the courts in response to these threats to ensure adequate data security standards.[187] Cloud computing data breaches target victims across many sectors and industries like retail, healthcare and government. However,

[184] S Sean "Governing Cyberspace: The Need for an International Solution" (1997) 32 *Gonzalez Law Review* 376.
[185] C Bennett and C Raab *The Governance of Privacy: Policy Instruments in Global Perspective* (2006) 276.
[186] Bennett *The Governance of Privacy: Policy Instruments in Global Perspective* 283.
[187] M A Reetz, L B Prunty, G S Mantych and D J Hommel "Cyber Risks: Evolving Threats, Emerging Coverages, and Ensuing Case Law" (2018) 122 *Penn State Law Review* 727 at 758.

the financial services sector is mainly targeted the most because it maintains extensive customer and consumer financial data.[188]

Despite the numerous technical benefits of cloud computing, consumers must consider the significance of what legal rights and responsibilities these new technologies trigger.[189] As with most new technologies, the applicability of existing laws, the possibility of new laws tailored for new technology such as cloud computing and big data, and the spectre of future regulatory action remain unclear.[190] Although the modern world has shifted to a global economy, cloud computing reaches every corner of the globe.

Service providers' management structures are forced to balance the reward of investing in new technologies with the risks posed by lawsuits under existing laws in the context of cloud computing.[191] The possibility that their firm will be exposed to significant new and unforeseeable liabilities under future laws and regulations are imminent. In most cases, large companies looking to utilise cloud computing must rely mostly on skilled contract writing rather than clear industry or government-enforced standards to protect their rights and liabilities.[192] The individuals and smaller companies are essentially unable to negotiate and are thus subject to adhesion contracts with whatever terms the various service providers include.[193]

In most countries, organisations and corporations are advised to negotiate their contracts and terms of service. A none negotiable service agreement is the standard in publicly available cloud computing.[194] These contracts should include clauses such as jurisdictional choice and time limits for the effective assumption of remedial

---

[188] *Ibid*.

[189] R Nichols "Cloud Computing by the Numbers: What do All the Statistics Mean?" (31 August 2010) *Computer World* http://blogs.computerworld.com /16863/cloud-computing -by-the-numbers-what-do-all-the statistics mean (Accessed 7 July 2020). Cloud computing services take advantage of the principles of economies of scale and specialization to provide a more efficient solution for many information technology problems and Ryan 2014 *Santa Clara Law Review* 513.

[190] Ryan 2014 *Santa Clara Law Review* 498.

[191] J McKendrick "Cloud Computing Market Hot, but How Hot? Estimates are All Over the Map" (13 February 2012) *Forbes* 2 http://www.forbes.com/ sites/joemckendrick/2012/02/13/ (Accessed 07 July 2020).

[192] Ryan 2014 *Santa Clara Law Review* 498.

[193] *Ibid.*

[194] Ryan 2014 *Santa Clara Law Review* 516.

action.[195] The maze of laws and regulations facing the cloud computing industry is generally attached to the right of privacy, security and jurisdictional components such as the GDPR, EU–US Privacy Shield, C 4176 of 2016 and the POPI Act.[196]

2.7 Jurisdiction for cloud computing regulation

One of the challenges in cloud computing refers to defining the concept of state jurisdiction in cyberspace. Territorial Jurisdiction is the most affected area of international law by cyberspace.[197] One of the reasons is that it is difficult to ascertain the meaning of state jurisdiction in cyberspace is the Internet's borderless nature.

Traditionally, state jurisdiction has been established by relying primarily on territorial criteria, such as exercising jurisdiction over acts committed within its territory and those established within its borders.[198] However, the acts committed online happen in a *prima facie* non-physical environment. It is not always possible to identify both the perpetrator of an unlawful act and the territory in which it originated.[199] It is also equally unclear where the unlawful act produced its adverse effects.[200] Because of these reasons, it is difficult to establish which state would be entitled to apply its laws to regulate acts committed online.

The use of cloud computing involves the flow of data across multiple jurisdictions, as mentioned above, therefore, the legislation must contain applicable law and its jurisdictional reach.[201] The purpose of the jurisdictional provision is to ensure the application of data protection of the citizens' personal information.[202] The jurisdictional

---

[195] S Bradshaw *et al* "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services" (2011) 19 *International Law Journal and Information Technology* 187 at 198 to 214.

[196] N S Gil "What is the Sword of Damocles?, Classical History" http://ancienthistory.about.com / od/ciceroworkslatin/flDamoclesSword.htm (Accessed 30 May 2020).

[197] M Hayashi "Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace" (2006) 6 *International Law Journal* 284.

[198] *Ibid* and R Uerpmann-Wittzack "Principles of International Internet Law" (2010) 11 *German Law Journal* 1245 at 1253.

[199] Hayashi 2006 *International Law Journal* 284 and Uerpmann-Wittzack 2010 *German Law Journal* 1253.

[200] *Ibid.*

[201] Hon 2012 *International Review of Law Computers and Technology* 132.

[202] *Ibid*.

provisions should also be enforceable when data is remotely processed in another country or a third country to another country.[203]

With most companies adopting cloud computing, each country establishes its data protection laws and mechanisms to guarantee stability, such as the POPI Act, the GDPR and the Indian Information Technology Act of 2000 (IIT Act). Research indicates that more than half of the USA companies are already using cloud computing to process personal information.[204]

The individual protection regimes adopted by the governments must also establish extraterritorial jurisdiction under international law.[205] The extension of extra-territorial controls on data protection laws could create concerns because state sovereignty could be undermined or compromised in the process. Sieber and Neubert stated that ever since the famous Trail Smelter Arbitration, it has been an accepted principle in international law that acts attributable to a state that is conducted from the territory of one state, but that takes effect within the territory of another state infringe the sovereignty of the affected state.[206]

The role of digital and information technologies in the generation of national wealth now means that the new risks associated with these changes require continued attention on all parties; national, regional and international.[207]

---

[203] *Ibid.*

[204] R Cohen "The Cloud Hits the Mainstream. More than half of the US Businesses Now Use Cloud Computing" (16 April 2013) *Forbes* http://www.forbes.com/sites/reuvencohen 2013/04/16/ (Accessed 09 April 2020).

[205] Narayanan 2012 *Chicago Journal of International Law* 790.

[206] U Sieber and C W Neubert "Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty" (2017) *Max Planck Yearbook of United Nations Law* at 257 and N Seitz "Transborder Search: A New Perspective in Law Enforcement" (2005) 7(1) *Yale Journal of Law Technology* 24 at 36 ("A trans-border search brings about physically perceptible changes to the outside world in the territory of the third country because data processing is initiated on servers that are located in the foreign state . . . It cannot make a difference whether the acting officer is physically present at the foreign site of the server when undertaking the measure or whether he accesses the server over the internet or, in some cases, also over an intranet. The result of his activity is the same in both cases: data processing is initiated on servers located in foreign territory. The decisive criterion to answer the question of whether or not a violation of the principle of territoriality occurs is thereafter not the physical presence in foreign sovereign territory but whether the measure causally precipitates a perceptible change in the outside world in the foreign territory").

[207] Broadhurst 2006 *Policing: International Journal of Police Strategies and Management* 408.

2.7.1 Extraterritorial jurisdiction under international law

Territorial jurisdiction is the most fundamental and commonly accepted exercise jurisdiction to prescribe in criminal matters. There are various international, regional, and national instruments aimed to enhance the fight against the protection of personal information. They all rely on territoriality as the primary basis for exercising jurisdiction.[208]

The existing legal frameworks have portrayed inadequacy in dealing with data breaches in the past.[209] The use of cloud computing and criminal activities in relation to it can be controlled by framing legal rules, strengthening the administrative framework, and convicting the accused following the quick and efficient justice delivery system. The judiciary throughout the world has been dealing with these problems already long before the introduction of cloud computing.[210]

Every state can extend their jurisdiction under international law when regulating data protection in the context of cloud computing.[211] This type of system is predicated on an international law regime buttressed by the case of *SS Lotus France v SS Bozkourt Turkey.*[212] In this case, the Permanent Court of International Justice (PCIJ) determined no restriction on states' exercise of jurisdiction unless there is international law prohibiting such an exercise.[213] Since cloud computing represents a brand new frontier

[208] African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) EX.CL/846(XXV) 2014, Computer Crime and Cybercrime, Southern African Development Community (SADC) Model Law 2013, Council of Europe, Convention on Cybercrime, Budapest 23 November 2001, ETS No. 185, Art. 22(1)(a), Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, Strasbourg, 28 January 2003, ETS No. 189, Art. 4(1), Arab Convention on Combating Information Technology Offences, Cairo, 21 December 2001, Art. 30(1)(a), Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2001 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography and Replacing Council Framework Decision 2004/68/JHA (2011) OJ L 335, Art. 17(1)(a), Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA (2014) OJ L 218, Art. 12(1)(a), GDPR, POPI Act and Cybercrimes Act.

[209] Sony "Data Security in the Cloud" 3.

[210] A Deb "Cyber Crime and Judicial Response in India" (2012) 3 *Indian Journal of Law and Justice* 106.

[211] Narayanan 2012 *Chicago Journal of International Law* 789.

[212] 1927 PCIJ (ser A) No 10 para 10 and H P Aust *Complicity and the Law of State Responsibility* (2011) 67 to 68.

[213] *Ibid*.

for international law, the principle that everything that is not expressly forbidden is allowed seems more acceptable and perhaps even essential.

Data protection is a mixture of private and public law. Under certain circumstances, some provisions may apply under one of the wings or both.[214] Criminal and competition laws are an example of public law. International private laws such as the law of damages and property law are mainly determined by the conflict of laws within agreements and contracts.[215] It is neither useful nor necessary to analyse the regulation to determine under which provisions are public and which ones are private.[216]

It is for jurisdictions that are necessarily influenced by Article 403 of the Restatement of Foreign Relations Law to use this determination in what law applies.[217] This section provides that a state may not exercise jurisdiction to prescribe law for a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable.[218]

Under international law in cloud computing, various legal territorial principles need to be considered. These principles would provide guidelines regarding the applicable law in some instances and determine the jurisdiction and remedial enforcement mechanisms on data breaches occurring in the host country of the responsible party.

These territorial principles are the subjective territorial principle and the objective territorial principle. They also include jurisdiction based on the nationality of the data subject, data protection against foreign data breaches that cause injury to nationals of that state and the protective territorial principle. Each principle will be discussed below

---

[214] C Kuner "Data Protection Law and International Jurisdiction on the Internet Part 1" (2010) 18 (2*) International Journal of Law and Information Technology* 176 at 181 to 183.

[215] Narayanan 2012 *Chicago Journal of International Law* 790.

[216] *Ibid.*

[217] K Hixson "Extraterritorial Jurisdiction Under the Third Restatement of Foreign Relations Law of the United States" (1988) 12(1) *Fordman International Law Journal* 127 and American Institute Restatement of the Law Third: The Foreign Relations Law of the United States http://www.ali.org/publications/show/foreign-relatios-law-united-states-rest/ (Accessed 09 April 2020).

[218] Article 403 of the Restatement (Third) of US Foreign Relations Law of 1986.

in the context of cloud computing regulation in light of international law and extraterritorial application of the law.

2.7.1.1 Subjective territorial principle

All the sovereign states have the power to prescribe public law in their territories without fear, favour, prejudice or interventions from other states or international bodies.[219] With technological growth, migration and globalisation, there have been a number of extensions of this principle. Countries revise their legislating powers in response to other states' inadequate adjudication of certain matters, such as the processing of personal information.[220]

The subjective territorial principle extends jurisdiction to activities commenced within a state's geographical territory but completed or consummated in other territories.[221] Traditionally, subjective territoriality relies upon four main aspects. Firstly, criminal conduct, which is the data breach or unlawful processing of personal information, took place. The location is the most useful place where evidence to solve a crime is found.[222] The second aspect is where the perpetrator engaged in the criminal conduct; this would possibly be the place where most of the witnesses of criminal activity are likely to be.[223]

The third aspect is to ensure due process and compliance with the legality, according to which individuals must be warned that a certain act is criminalised.[224] Contrary to the place of result, which may be random and unpredictable, the place of conduct is more or less always certain.[225] The fourth aspect is the idea that, from a criminological point of view, it is more important for states to sanction the expression of a criminal will on their territory than to protect and restore their public order.[226] According to Foucault, territorial jurisdiction aims to re-establish a balance on its extreme point, the

---

[219] Kuner 2010 *International Journal of Law and Information Technology* 181 to 183.
[220] B E Carter *et al International Law* 5th Edition (2007) 657 to 658.
[221] Narayanan 2012 *Chicago Journal of International Law* 791 and G Gilbert "Crimes Sans Frontières: Jurisdictional Problems in English Law" (1993) 63(1) *British Yearbook of International Law* 1 at 430.
[222] H Donnedieu de Vabres *Treaty on Criminal Law and Comparative Law* 3rd Edition (1947) 927.
[223] *Ibid*.
[224] *Ibid*.
[225] A Huet and R Koering-Joulin *International Criminal Law* 3rd Edition (2005) 226.
[226] Donnedieu de Vabres *Treaty on Criminal Law and Comparative Law* 927.

connection between the party who violated the law and the all-powerful sovereign who displays his strength.[227]

This form of territorial jurisdiction is not widely accepted as a general principle; however, the Restatement of Foreign Relations Law leaves room for its expanded application.[228]

The first reason explaining the inadequacy of subjective territorial principle in cloud computing is its technical nature. This relates to difficulties tracing the origins of the perpetrators and identifying where the criminal conduct of a data breach took place.[229] Each computer system, such as desktops, smartphones and tablets connected to the Internet, is assigned a unique Internet Protocol (IP) address.

The IP address consists of four IPv4 to six IPv6 numbers, between 0 and 255.[230] These IP addresses are managed globally by the International Corporation for Assigned Names and Numbers (ICANN).[231] ICANN does not run the system, but it helps coordinate how IP addresses are supplied to eliminate the repetition of IP addresses. ICANN is also the central repository for IP addresses, from which ranges are provided to the five Regional Internet Registries (RIRs).[232] The RIRs are responsible in their designated territories for assigning to end-users and local internet registries, such as Internet service providers.[233]

---

[227] M Foucault *Discipline and Punish: The Birth of the Prison* (1995) 48 to 49.

[228] International Convention for the Suppression of Counterfeiting Currency (1929) 112 League of Nations Treaty Ser 371 (1931) and the Convention of 1936 for the Suppression of the Illicit Traffic in Dangerous Drugs (1936) 198 League of Nations Treaty Ser 301 (1939).

[229] Communication from the European Commission to the Council and the European Parliament "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, COM" (2012) 0140 final Brussels 3.

[230] K Shaw "What is IPv6, and Why Are We Not There Yet?" (27 September 2018) *Network World* https://www.networkworld.com (Accessed 12 July 2020) (IPv6 addresses were developed in 1995, and standardised in 1998) and S Hoog and E Vyncke "Introduction to IPv6" (19 December 2008) *Cisco Press* https://www.networkworld.com (Accessed 12 July 2020).

[231] *Ibid.*

[232] RIPE Network Coordination Centre "What We Do" https://www.ripe.net/ what-we-do (Accessed 12 July 2020) and NRO "Regional Internet Registries" https://www.nro.net (Accessed 12 July 2020) (There are currently five RIRs: RIPE-NCC (Europe and the Middle East), ARIN (North America), APNIC (Asia-Pacific), LACNIC (Latin America and Caribean) and AfriNIC (Africa).).

[233] *Ibid.*

In the context of cloud computing, considering that the IP address of a computer points at a physical address,[234] determining the place of origin of the data breach does not seem to raise any technical issue. It merely consists in identifying the IP address of the computer system used by the perpetrator. However, the problem is that perpetrators usually would not make any intrusion directly from their IP address.[235] They find a way to conceal their IP addresses to engage in criminal conduct. There is a range of techniques, software programs, and websites accessible over the Internet, allowing individual users to hide who or where they are.[236]

Usually, the perpetrator of data breaches can easily replace the IP address of the computer system so that the offence is presumed to come from a location other than the one from which it truly stems.[237] This is due to the consideration that there are many open proxies on the Internet that anyone can access.[238] This technique is called IP spoofing, and it is easy to implement.[239]

Another technique is using proxy servers, public or private, which enables connection to a network via an intermediary server to conceal their online activity.[240] This is the most commonly used method to hide the geographical origin of an offence committed on cloud computing. It takes control over a remote computer system in a foreign country and then uses that computer as a staging tool from which to perpetrate the offence.[241]

---

[234] Gilbert *Crimes Sans Frontières: Jurisdictional Problems in English Law* 387.

[235] P Rosenzweig "Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World" (2013) *Santa Barbara Praeger Security International* 78.

[236] D J Davies "Criminal Law and the Internet: The Investigator's Perspective: Crime, Criminal Justice and the Internet" (1998) *Criminal Law Review Special Edition* 1 at 53.

[237] Rosenzweig 2013 *Santa Barbara Praeger Security International* 78 and H F Lipson "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues" (2002) *Carnegie Mellon Software Engineering Institute* 14 https://resources.sei.cmu.edu/asset_files/SpecialReport/2002_003_001_13928.pdf (Accessed 11 July 2020).

[238] J A Muir and P C Van Oorschot "Internet Geolocation and Evasion" (2009) 4 *ACM Computer Survey* 1 at 15.

[239] *Ibid*.

[240] C S D Brown "Investigating and Prosecuting Cybercrime: Forensic Dependencies and Barriers to Justice" (2015) 9(1) *International Journal of Cyber Criminology* 55 at 80 and Muir 2009 *ACM Computer Surve*y 14.

[241] *Ibid.*

This targeted computer system, used to conceal the geographical location, is often the last link in a long chain involving numerous computer systems and jurisdictions.[242] By moving data from one computer system to the next, perpetrators can conceal the true origin of the data breach, making tracking and tracing a problematic task.[243] Countries such as China and India are convenient targets because of the large number of computer systems that outsiders from around the world can easily compromise as their target to conceal the actual geographical location of the data breach.[244]

The second challenge is that of consent. Consent from the state where the data are physically located can be obtained in two ways. Firstly, consent can be obtained on a case-by-case basis.[245] However, due to the number of jurisdictions to contact, the problem is that the legal process to obtain consent is usually time-consuming, which is incompatible with the volatile nature of data.[246] Secondly, consent can be granted in advance by virtue of a treaty provision, such as Article 40 of the Arab Convention on Combating Information Technology Offences or Article 32(b) of the Convention on Cybercrime.[247]

In a significant development for US law enforcement's ability to access data stored abroad, the US Congress enacted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) at the end of March 2018.[248] The Act enables US law enforcement to compel Internet service providers based in the US and subject to the Stored Communication Act (SC Act)[249] to hand over data. The CLOUD Act applies whether

---

[242] *Ibid.*

[243] Lipson "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues" 19, J B Maillart "The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime"(2018) 19 *ERA Forum* 378 to 379 https://doi.org/ 101007s12027-018-0527-2 (Accessed 12 July 2020) and S W Brenner "Toward a Criminal Law for Cyberspace: Product Liability and Other Issues"(2004) 1 *Pittsburgh School of Law Journal of Technology Law* 1 at 14.

[244] *Ibid*.

[245] *Ibid.*

[246] J J Schwerha "Law: Law Enforcement Challenges in Trans-border Acquisition of Electronic Evidence from Cloud Computing Providers" (2010) *Council of Europe Discussion Paper* 18 https://rm.coe.int/16802fa3dc (Accessed 10 July 2020).

[247] Arab Convention on Combating Information Technology Offences.

[248] The US Stored Communications Act, 18 U.S.C. § 2701 (SC Act) applies to an 'Electronic Communications Service provider,' as defined in 18 U.S.C. Crimes and Criminal Procedure 2510(15), and a 'Remote Computing Service,' as defined in 18 U.S.C. Crimes and Criminal Procedure 2711(2).

[249] The US Stored Communications Act, 18 U.S.C. § 2701.

that data is located within or outside the US by adding extraterritoriality provision to the SC Act. Some of these provisions state that:

> "…the service provider preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States".[250]

The adoption of the CLOUD Act by the US assisted the US Supreme Court to decide on the Microsoft Ireland courts case that it was set to resolve *United States v. Microsoft Corp*.[251] This case involved a dispute between Microsoft and the US government regarding the extraterritorial reach of the SC Act. More specifically, the issue was whether a warrant obtained under the SC Act could compel a US company to produce information under its control but stored outside the US.

The government argued that its warrant authority required US-based service providers to turn over responsive data, regardless of where these data happened to be held. Microsoft, by contrast, argued that this authority only extended to data located within the territorial boundaries of the US. Microsoft believed that the US could not compel production via a US-issued warrant if the data were stored abroad.[252] Instead, it would be required to make a Mutual Legal Assistance (MLA) request and rely on the foreign government to access the data and turn it back to the US.

After the CLOUD Act's enactment, the US obtained a new warrant seeking the emails at issue in its dispute with Microsoft under the authority of the new law.[253] Because both the US and Microsoft agreed that the new warrant replaced the prior warrant, the

---

[250] The US Clarifying Lawful Overseas Use of Data Act (CLOUD Act) 103(a)(1) and 18 U.S.C. Crimes and Criminal Procedure subsection 271.
[251] No. 17-2, 548 U.S. 2018 WL.
[252] *Ibid.*
[253] *United States v Microsoft Corp*., No. 17-2, 548 U.S. 2018 WL 1800369, slip op. para 2 (U.S. April 17, 2018).

Supreme Court concluded on 17 April 2018 that the case had become moot and vacated the lower court's rulings with instructions to dismiss.[254]

Certain countries may find that the subjective territorial principle provides a strong jurisdictional basis to bind cloud computing service providers to their cloud computing regulations.[255] Regarding the adequacy measure of regulation, when there is harm related to data breaches, states can use the entire chain of data processed between servers to identify specific locations of servers that do not abide by the given adequacy measure.[256] Once identified, the injured data subject could extend that country's jurisdiction to the cloud computing service provider controlling the rogue server. This is done under the theory that their inadequate protection began processing data from the user in the injured country. [257]

However, concerns over data protection regarding cloud computing, as discussed above, necessarily require that data freely move across borders.[258] The goal of cloud computing regulation is to ensure that the cloud computing service providers cannot escape the onus of an adequacy measure or a right to access by moving data across borders.[259]

2.7.1.2 Objective territorial principle

In terms of the objective territorial principle, the state's jurisdiction is extended to acts committed in another state's territory.[260] These acts should either be (a) consummated or completed in the territory of the state extending jurisdiction or (b) produce harmful consequences in the territory of the party extending jurisdiction such as identity theft.[261] The objective territorial principle also extends further to provide the effects doctrine.[262]

---

[254] *United States v Microsoft Corp.*, No. 17-2, 548 U.S. 2018 WL 1800369, slip op. para 2.
[255] Narayanan 2012 *Chicago Journal of International Law* 792.
[256] Rosenzweig 2013 *Santa Barbara Praeger Security International* 78 and Lipson "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues" 14.
[257] Maillart 2018 *ERA Forum* 378 to 379.
[258] *Ibid* and Mvelase 2013 *Conference paper* 149.
[259] *Ibid.*
[260] Carter *et al International Law* 661.
[261] *Ibid* and Narayanan 2012 *Chicago Journal of International Law* 792, Hayashi 2006 *International Law Journal* 284 and Uerpmann-Wittzack 2010 *German Law Journal* 1245.
[262] Carter *et al International Law* 662.

The effects doctrine suggests that jurisdiction arises when the effects of a particular activity are direct and so reprehensible in nature. Economic impacts, social unrest, or political instability can necessitate such jurisdiction.[263] Under this principle, states are only justified using the effects doctrine when those effects are intended, direct and substantial.[264] Though similar to the effects doctrine, this heightened standard demanding that effects be more closely tied to the state extending jurisdiction is crucial in determining the breadth and scope of cloud computing regulation.[265]

The international renowned IT organisation, Yahoo!,[266] also went through various court procedures based on the internet activities emanating from the company database and website. One of the cases involved the racial content posted and published on the Yahoo! web page. In this case,[267] the dispute centred on Nazi-related items available on the Yahoo! auction site, allegedly in violation of a provision in the French penal code of 2005[268] prohibiting the selling of such items.

The Tribunal de Grande Instance (TGI) found that French courts had jurisdiction because the placement of items for sale caused damage to be suffered by *La Ligue Contre le Racisme et L'Antisemitism* (LICRA) and '*Union des Etudiants Juifs d*e

[263] Carter *et al International Law* 663.
[264] P L C Torremans "Extraterritorial Application of E.C and U.S. Competition Law" (1996) 21 *European Law Review* 280 at 284.
[265] Torremans 1996 *European Law Review* 288.
[266] Yahoo! Inc. was founded in 1994 by two PhD candidates in electrical engineering at Stanford University to keep track of their favourite websites on the Internet. Originally named "Jerry's Guide to the World Wide Web" after co-founder Jerry Yang, the founders changed the name to Yahoo!. The Yahoo! name is an acronym for "Yet Another Hierarchical Officious Oracle," but the co-founders insist they chose the name because they liked its dictionary definition as meaning a person who is "rude, unsophisticated, uncouth." "The History of Yahoo-How It All Started" *Yahoo! Media Relations* http://docs.yahoo.comlinfo /misclhistory.html (Accessed 02 July 2020).
[267] *UEJF v Yahoo! Inc TGI Paris Ordonnancede* R6f6 Nos 00/05308, 00/05309 TGI Paris, 22 May 2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France*, http://juriscom.net /2000/05/tgi-paris-refere-22-mai-2000-uejf-et-licra-c-yahoo-inc-et-yahoo-france/ (Accessed 10 July 2020) and M H Greenberg "A Return of Lilliput: The *LICRA v Yahoo!* Case and the Regulation of Online Content in the World Market" (2003) *Berkeley Technology Law Journal* 1191 to 1192.
[268] French Criminal Penal Code of 2005 01/01/2005 https://www.legal-tools.org /doc/418004 (Accessed 11 July 2020), CODE PENAL [C. PEN.] art. R.645-1 (Fr.) Translation available online at http://www.lex2k.org/yahoo/ art645.pdf (Accessed 11 July 2020), Sub-section 130(1)(3) STRAFGESETZBUCH [StGB] (F.R.G.) and Section 130(3) of the Federal Criminal Code in Germany provides that "Imprisonment, not exceeding five years, or a fine, will be the punishment for whoever, in public or in an assembly, approves, denies or minimizes (the Holocaust) committed under National Socialism, in a manner which is liable to disturb the public peace." Sub-section 130(1)(3) StGB (F.R.G.).

France (UEJF). These are the two French organisations dedicated to fighting anti-Semitism.[269] Since both of these organisations were in France, the Tribunal reasoned that France had jurisdiction to hear the case. On appeal, Yahoo! claimed that France did not have jurisdiction because all of the elements that made up the offence in question were committed outside of France.[270] However, the Tribunal concluded that because the content was available in French territory through the Internet, the elements materialised both abroad and in France.[271]

In the court order of 22 May 2000, the TGI established jurisdiction over the case pursuant to article 46 of the Code of Civil Procedure. Article 46 establishes that in matters of delict or damages, a plaintiff may bring a case before the court of the place of the event causing liability or the one in whose jurisdiction the damage was suffered.[272]

Judge Jean-Jacques Gomez found that making it possible for users in France to access a website where Nazi memorabilia were displayed for sale equated to committing a wrong within the French territory that produced harm in France.[273] The judge, therefore, accepted LICRA and UEJF claims and ordered Yahoo! Inc. to take all necessary measures to dissuade and render impossible from within the French territory any access via Yahoo.com to the Nazi artefact auction service and to any other site or service that may be construed as constituting an apology for Nazism or a contesting of Nazi crimes.[274] Yahoo France was further ordered to issue all the Yahoo

[269] *Yahoo! Inc v La Ligue Contre Le Racisme Et L'A.ntisemiisme* 433 F3d 1199, 1225 (9th Cir 2006).
[270] Hayashi 2006 *International Law Journal* 292 to 293.
[271] Hayashi 2006 *International Law Journal* 293.
[272] Art. 46 nouv. C. pr. civ, English translation https://www.legifrance.gouv.fr/content/download/1962/13735/version/3/.../Code_39.pdf (Accessed 10 July 2020).21
[273] *Yahoo! Inc. v La Ligue Contre LeRacisme et L'Antisemitisme* 169 F. Supp. 2d. 1181 (N.D. Cal. 2001) (No. 00-21275) "Whereas while permitting these objects to be viewed in France and allowing surfers located in France to participate in such a display of items for sale, the Company YAHOO! Inc. is therefore committing a wrong in the territory of France … Whereas, the damage being suffered in France, our jurisdiction is therefore competent to rule on the present dispute under Section 46 of the New Code of Civil Procedure' 1208-1209" citing Pl.'s Compl. for Decl. Relief, ex. A, 5 to 6.
[274] *Yahoo! inc v La Ligue Contre le Racisme et l'Antisemitisme et al*, 169 F. Supp. 2d 1181 (N.D. Cal. 2001) http://law.justia.com/cases/federal/district-courts/ FSupp2/169/1181/2423974/ (Accessed 10 July 2020).

Internet users a warning to seize their search on Yahoo.com and was provided with search results that included sites that violated the French penal code.[275]

In the context of cloud computing, with the understanding of the effects doctrine, one may determine whether this adoption of the objective territorial principle may be used to provide jurisdiction for cloud computing regulation. In the event of data breaches, the state seeking to extend jurisdiction would argue that the harm suffered was an effect of the violation, even if that act was committed wholly outside of French territory.[276]

Under this reasoning, a failure either to meet adequacy standards or to provide rights to data breaches causing economic harm to individuals or business entities in the state implicates the regulation. This argument is supported by the facts in the case of *Dow Jones and Company Inc v Gutnick.*[277] This case was decided in December 2002 by the High Court of Australia (HCA). The case was based on defamation.

The proceedings were brought before the Supreme Court of Victoria (SCV) in October 2000 by Mr Gutnick, an Australian businessman and resident. Mr Gutnick sought compensation for damage to his reputation that he alleged had happened in Victoria. He alleged that the harm to reputation was caused by publishing a defamatory article by the US-based Dow Jones on the subscription website WSJ.com. The alleged defamatory article was published in *Barron's Online* journal. Dow Jones applied to Hedigan J from the Supreme Court of Victoria, asking for the proceedings to be set aside and any further proceedings on the matter to be stayed.[278]

Dow Jones claimed that the Supreme Court of Victoria did not have jurisdiction to hear the case as the publication of the allegedly defamatory article happened in New Jersey in the US. The article was allegedly uploaded on the Dow Jones' servers in New

[275] *Yahoo! inc v La Ligue Contre le Racisme et l'Antisemitisme et al*, 169 F. Supp. 2d 1181.
[276] *United States v Alcoa* 148 F2d 416 at 443-44 (2d Cir 1945) and *Harford Fire Insurance Co v Calfornia* 509 US 764, 798 (1993) (Holding that international community does not stop the exercise of jurisdiction).
[277] (2002) 210 CLR 575.
[278] *Dow Jones and Company Inc v Gutnick* (2002) 210 CLR 575 para 5.

Jersey. Hedigan J dismissed Dow Jones' appeal since he found that the defamation of Mr Gutnick had happened in Victoria. It was in Victoria where the article could be downloaded and therefore accessible by readers.[279] The Court of Victoria dismissed Dow Jones's appeal and upheld the primary judge's decision.[280]

Therefore, the case was brought to the High Court of Australia (HCA). In its judgement, the HCA explained that Australia's common law requires the judges to apply the law where the delictual damage occurred. The judges then explained the main elements of the delict. They stated that defamation is defined as damage to reputation due to the publication of defamatory material under Australian law. The HCA also added that the delict is usually located where the damage to reputation occurs. In addition, the judges clarified that since the "actionable wrong" is the damage to reputation, for defamation to exist, not only does the material have to be published, but it must also be made available to the reader in comprehensible form.[281]

This is because it is only when a third party comprehends the material that the damage to reputation occurs.[282] The Court specified that publication of defamatory material must be interpreted as a bilateral act in which the publisher makes it available, and a third party has it available for their disposal.[283] Therefore, the Court found that the respondent's claim that the damage to his reputation had happened in Victoria was correct. The court further stated that Mr Gutnick had a reputation in Victoria and in Victoria, the material published online could be downloaded and comprehensible to readers. It is where that person downloads the material that the damage to reputation may be done.[284]

The two cases examined in the previous paragraphs outline the difficulties that national courts face when establishing jurisdiction on Internet related disputes over defendants located outside the domestic forum. As mentioned above, the national courts in these cases faced the same challenge: establishing when an act committed

[279] *Dow Jones and Company Inc v Gutnick* (2002) 210 CLR 575 para 2.
[280] *Dow Jones and Company Inc v Gutnick* (2002) 210 CLR 575 para 2.
[281] *Dow Jones and Company Inc v Gutnick* (2002) 210 CLR 575 para 25.
[282] *Dow Jones and Company Inc v Gutnick* (2002) 210 CLR 575 para 26.
[283] *Dow Jones and Company Inc v Gutnick* (2002) 210 CLR 575 para 26.
[284] *Dow Jones and Company Inc v Gutnick* (2002) 210 CLR 575 para 44.

online by defendants located in another state can be said to have happened within the domestic court's jurisdiction.

In terms of the objective territorial principle, a failure to provide adequate data protection laws and standards that might cause harm to individuals or business entities in the state implicates the regulation.[285] The existing applications of international law suggest that a state has jurisdiction over activities abroad that cause measurable harmful effects in that state.[286]

2.7.1.3 Jurisdiction based on the nationality of the data subject

Every state is mandated to protect its citizens from any kind of harm that could jeopardize the well-being of its citizens and inhabitants. The power of states to prescribe laws covering the activities of their nationals is important.[287] This principle provides that the states can prescribe cloud computing regulations for their nationals at home or abroad.[288] It is based on the assumption that a person grants the country of which he is a national the right to regulate his conduct, no matter where they are located geographically.[289]

Under international law, nationality jurisdiction extends to corporations in which states have a sufficient amount of equity.[290] However, considering that the largest cloud computing providers are US entities such as Amazon and Google, the limitation on nationality jurisdiction would constrain the US's ability to prescribe cloud computing regulations for all world users of these cloud computing services. Limiting the US's extraterritorial jurisdiction in this way prevents the US from dictating the relevant terms of a global cloud computing regulatory scheme. If these cloud computing service providers want to have subsidiaries in the countries they service, those corporations would be subject to the host country's laws and regulations of data protection.[291]

---

[285] Narayanan 2012 *Chicago Journal of International Law page* 795.
[286] *Ibid.*
[287] Section 402(2) of Restatement (Third) of USA Foreign Relations Law.
[288] Narayanan 2012 *Chicago Journal of International Law* 795.
[289] S Wilske and T Schiller "International Jurisdiction in Cyberspace: Which States May Regulate the Internet?" (1997) 50 *Federal Communications Law Journal* 117 at 131.
[290] Wilske 1997 *Federal Communications Law Journal* 131.
[291] C D Wallace *The Multinational Enterprise and Legal Control: Host State Sovereignty in an Era of Economic Globalisation* 15th Edition (2002) 602 to 605.

2.7.1.4 Data protection against foreign data breaches that cause injury to nationals of that state

This is also referred to as the passive personality principle. It allows the state to exercise jurisdiction over an act committed by an individual outside of its territory because the victim is one of that country's nationals.[292] The passive personality principle is based on the duty of a state to protect its nationals abroad.[293] Under this principle, the sovereignty asserting jurisdiction is concerned with the effects of data breaches rather than where it occurs.[294] The passive personality principle is the most controversial of the five accepted bases of jurisdiction in international law.[295]

This principle is frequently applied in response to terrorist attacks as opposed to cloud computing specifically.[296] The challenge of using this principle to justify extraterritorial jurisdiction for cloud computing regulation is determining whether this principle could reasonably be extended outside the criminal context. The other challenge of this principle is whether the injuries that may result from inadequate data protection could be classified as the harm that justifies protection under this principle.

However, international law would likely not support its use in this context, some of the incidents that could cause a company to lose profits due to data breaches.[297] Other data breaches could have this principle applicable, for example, violations of individuals' privacy. This is a principle recognised by the United Nations (UN) as a fundamental human right.[298] However, one could argue that jurisdiction for cloud computing regulations under this principle would arise on a case-by-case basis when the resulting data breaches are significant enough.

---

[292] Research in International Law Under the Auspices of the Faculty of the Harvard Law School "Jurisdiction with Respect to Crime" (1935) 29 *American Journal of International Law* 443 at 445 (The principle is usually used only to gain jurisdiction over the acts of a foreigner abroad; however, theoretically it can be used to acquire jurisdiction over the acts of a nation abroad. Thus, there may be an overlap between the passive personality and nationality principles).

[293] *Ibid* and G Gilbert *Responding to International Crime* 2nd Edition (2006) 88 to 90.

[294] J G McCarthy "The Passive Personality Principle and Its Use in Combatting International Terrorism" (1989) 13(3) *Fordham International Law Journal* 298 at 299 to 301.

[295] McCarthy 1989 *Fordham International Law Journal* 301.

[296] *Ibid.*

[297] Narayanan 2012 *Chicago Journal of International Law* 799 and McCarthy 1989 *Fordham International Law Journal* 300.

[298] International Covenant on Civil and Political Rights Art 17, 999 UN Treaty Ser 171 (1966) ICCPR.

Moreover, it might be challenging to determine precisely where data breaches occur. For example, when data is transferred through multiple servers across different jurisdictions, the country where the service is incorporated may not have great incentives to bring actions against the responsible party. Therefore, cloud computing regulations may be an ideal application of the passive personality principle.

2.7.1.5 The protective principle

Nonetheless, the countries that use the protective principle to extend jurisdiction against responsible parties may argue that those extraterritorial data breaches threaten the state's vital economic or security interests.[299] Thus, unlike some of the jurisdictional principles discussed above, the protective principle would allow states to extend jurisdiction. This extension should be without predicating that jurisdiction on the case's specific circumstances, such as whether there were harms associated with the activity or data breach. For this reason, since cloud computing is becoming sufficiently ubiquitous, the activities under the protective principle expand as well.

2.8 Challenges of cloud computing regulations

One of the constraints on a state's ability to regulate cloud computing emanates from a Word Trade Organisation (WTO) agreement concerning free access to services.[300] The WTO envisions a free trade system that allows the free supply of services across member states. This principle is reflected in the General Agreement on Trade in Services (GATS).[301]

Cloud computing service providers would undoubtedly fit into one of the supply modes that the GATS agreement purports to cover.[302] These cloud computing service providers may be described as providing services from one territory to another depending on how this kind of data transfer is characterised.[303] This is because cloud

[299] Narayanan 2012 *Chicago Journal of International Law* 800.
[300] Narayanan 2012 *Chicago Journal of International Law* 802.
[301] GATS (1994) 1869 UN Treaty Ser 183.
[302] Asinari "The WTO and the Protection of Personal Data. Do EU Measures Fall Within GATS Exception? Which Future for Data Protection within the IVTO E-Commerce Context?" 4.
[303] *Ibid*.

computing mechanism expands to the commercial trade sphere, such as the Amazon online purchasing platform. These economic activities draw consumers to the territory where the service providers are domiciled through cloud computing services. This indirectly creates the presence of the service provider in another territory to provide the cloud computing services to the data subject of another jurisdiction.[304]

Furthermore, because of the level of interconnectedness on which cloud computing depends, measures that are especially burdensome in one territory may make it infeasible or unprofitable to provide trans-border services in that area.[305] This forces customers to rely on national cloud computing service providers that do not move data across borders. The EU's GDPR, for example, includes a provision that requires an adequate level of protection of data before a data transfer to a third party outside of the EU; the SA's POPI Act also makes a similar provision.[306] The EU, South Africa or other jurisdictions with similar protections might argue that these regulations would be permitted under certain exceptions such as the responsible party in another state being subject to the binding corporate or binding agreements which provide an adequate level of data protection because the measures are specifically designed to protect privacy.

However, these exceptions mentioned above must be applied reasonably. Thus, the exception does not function as a carte blanche for states. They are still prohibited from providing more favourable treatment to regional cloud computing service providers over foreign ones.[307] This could only be applicable if the regulations are reasonably designed to protect individuals' privacy. Some commentators note that the GDPR and the POPI Act provisions may favour services from EU nations over US or other countries service providers in a way that would not be reasonable.[308]

[304] Narayanan 2012 *Chicago Journal of International Law* 803.
[305] *Ibid*.
[306] Article 44 of the General Data Protection Regulation and section 72 of the Protection of Personal Information Act.
[307] Asinari "The WTO and the Protection of Personal Data. Do EU Measures Fall Within GATS Exception? Which Future for Data Protection within the IVTO E-Commerce Context?" 2.
[308] *Ibid*.

The other constraint that seems to provide a lower bound to regulation is triggered by the United Nations (UN)'s International Covenant on Civil and Political Rights and its protection of a right to privacy.[309] The 2010 report from a UN Special Rapporteur assisted by the Office of the United Nations Human Rights High Commissioner, concerning the protection of privacy rights while countering terrorism, highlighted these constraints.[310] The report indicated the importance of a right to privacy on data protection by adopting data protection and privacy laws.[311] The report further stated that the laws adopted should ensure explicit legal protections for individuals to prevent the excessive processing and abuse of personal information.[312]

Though the crux of the report concerns government anti-terrorism measures such as wire-tapping, the right to privacy remained the actuating principle to reaffirm individual rights concerning their personal information. Moreover, the report noted that the right to privacy and data protection is emerging as a distinct human or fundamental right.[313] Because of this, it is reasonable to argue that even outside the terrorism context, this fundamental right requires a higher level of protection.

This level of protection also extends to the use of cloud computing to process personal information. Though the member states may not be required to comply with the recommendations of the Office of the High Commissioner concerning cloud computing regulations, the report suggests that the right to privacy at least requires a right to data protection as well.[314]

2.9 Conclusion

As different organisations and individuals continue to utilise cloud computing services in South Africa, more and more sensitive data are likely to be stored in the cloud.[315] South Africa is not immune to cyber-attacks in any form. However, the threat might not

[309] International Covenant on Civil and Political Rights (recognizing a right to privacy).
[310] M Scheinin "Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism" UN Human Rights Council 13th Session (2007) Agenda Item 3 UN Doc A/HRC/6/17 at 3.
[311] *Ibid*.
[312] *Ibid.*
[313] *Ibid.*
[314] *Ibid* and Narayanan 2012 *Chicago Journal of International Law* 804.
[315] *Ibid.*

rise to the level of a vital security interest in the form of terrorism. The individuals who utilise cloud computing services could reasonably argue that data security is of strong economic interest to the nation. Consequently, South Africa has to deem it necessary to extend extraterritorial jurisdiction even without an identified specific harm or potential data breach. In cloud computing, to process personal information, it is further crucial to look at the national data protection legal framework in South Africa. The following chapters will discuss these current legal frameworks in South Africa on data protection.

Chapter 3: The right to privacy under the common law and the Constitution in the cloud computing context

"…To deny people their human rights is to challenge their very humanity".[316]

3.1 Introduction

The use of cloud computing has raised concerns in relation to the right to privacy, as mentioned above. This is a right that has been recognised as a fundamental human right in a number of jurisdictions.[317] Privacy is associated with a recognised and protected right by both national and international law.[318] Some jurisdictions such as India, EU, South Africa and Cape Verde have adopted legislation on data protection in support of the constitutional protection of the right to privacy.[319]

This chapter focuses on the critical analysis of protecting the right to privacy in the cloud computing context under the SA legal framework. In this context, the relevant laws to consider are the common law and the Constitution. The analysis will determine whether these laws are sufficient to protect individuals from unlawful infringement of their right to privacy in the cloud computing context as a mechanism to process personal information. The last part will provide the concluding remarks of the chapter.

[316] Nelson Mandela, South African Former President and Civil Rights Activist (Updated 30 October 2015) *UCT Amnesty International* http://www.amnesty.org (Accessed 18 July 2020).

[317] Such as South Africa, Canada and Hungary as well as the Civil Organisations and the United Nations, F La Rue "Report of the Special Rappoteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression" (2013) UNHRC, 23rd Sess, Supp No 3, UN Doc A/HRC/23/40 at 6 and K N Rashbaum, B B Borden and T H Beaumont "Outrun the Lions: A Practical Framework for Analysis of the Legal Issues in the Evolution of Cloud Computing" (2014) 12(1) *AMLR* 71 at 753.

[318] M Barbaro "Government Interference with the Right to Privacy: Is the Right to Privacy an Endangered Animal" (2017) 6 *Canadian Journal of Human Rights* 127 at 133 and Y Onn "Privacy in Digital Environment" (2005) 7 *Haifa Centre of Law and Technology* 1, A Savoiu and C C Basarabescu "The Right to Privacy" (2013) *Annals Constantin Brancusi U. Targu Jiu Juridical Sci. Series* 89 and Rue "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression" 6.

[319] C Kuner "The European Union and the Search for an International Data Protection Framework" (2009) 2(2) *GroJIL* 55.

3.2 Definition and the scope of the right to privacy

The word privacy comes from the Latin *privare:* to deprive.[320] This term was adopted from the notion that a private person was somebody deprived of "an official position", absent from public life.[321] Privacy is a personality interest, and in turn, a personality interest can be described as a non-patrimonial interest that cannot exist separately from the individual.[322]

Privacy has many distinct definitions, and those definitions often shift in accordance with different generations, societies and contexts attached to it.[323] To define the concept of privacy, it is necessary to understand that every personality interest has a pre-legal existence in factual reality.[324] Since by nature, a person has a fundamental interest in particular facets of his personality such as his body, good name, privacy and dignity, these interests exist autonomously *de facto*, independently of their formal recognition *de jure*.[325] The right to privacy is the right to be left alone,[326] which was formulated by Samuel Warren and Louis Brandeis in 1890,[327] and the concept gained prominence since then.

The right to privacy is defined as the right that others do not possess undocumented personal information about the right holder.[328] Alan Westin, an early information

[320] Barbaro 2017 *Canadian Journal of Human Rights* 132.

[321] Barbaro 2017 *Canadian Journal of Human Rights* 133 and Onn 2005 *Haifa Centre of Law and Technology* 1.

[322] Neethling *et al Neethling's Law of Personality* 14 and A Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (LLD Thesis, UNISA, 2009) 545.

[323] rsonality 302 to 303, *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 271, *Jooste v National Media Ltd* 1994 (2) SA 634 (C) 645, *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T) 384, *Swanepoel v Minister van Veiligheid en Sekuriteit* 1999 (4) SA 549 (T) 553, *Motor Industry Fund Administrators (Pty) Ltd v Janit* 1994 (3) SA 56 (W) para 60 and *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) 462.

[324] J Neethling "The Concept of Privacy in South African Law" (2005) 122 *South African Law Journal* 18 at 19, J Neethling "The Right to Privacy, HIV/AIDS and Media Defendants" (2008) 125 *South African Law Journal* 36 at 37 and J Neethling "The Protection of the Right to Privacy Against Fixation of Private Facts" (2004) 121 *South African Law Journal* 519 at 519 to 520.

[325] Neethling 2005 *South African Law Journal* 19 and Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 545.

[326] *Curtis v Minister of Safety and Security and Others* 2000 (10) BCLR 1079 (CC) para 16, Savoiu 2013 *Annals Constantin Brancusi U. Targu Jiu Juridical Sci. Series* 91 and J C Nelson "Keynote Addresses: The Right to Privacy" (2007) 68 *Montana Law Review* 257 at 258.

[327] S Warren and L Brandeis "The Right to Privacy" (1890) 4 *Harvard Law Review* 193.

[328] W A Parent "Privacy, Morality, and the Law" (1983) 12 *Phil. and Pub. Aff.* 269, S C Rickless "The Right to Privacy Unveiled" (2007) 44 *San Diego Law Review* 773 at 774 and J Greene "Beyond Lawrence: Metaprivacy and Punishment" (2006) 115 *Yale Law Journal* 1862 at 1884.

privacy scholar, defined privacy as the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others.[329] The right to privacy has also been described as a broad value representing concerns about autonomy, individuality, personal space, solitude and intimacy.[330] According to Neethling, he defines privacy as a person's right to control their personal affairs and be reasonably free from unsolicited intrusions.[331]

In the early nineteen hundreds, the Transvaal Supreme Court in *R v Umfaan*[332] described the right to privacy as a personality right, which encompasses those real rights *in rem* related to personality, which every free man is entitled to enjoy.[333]

The concept of privacy should be sought in and defined in accordance with its existence and nature in factual reality. In this sense, privacy can be described as a condition of human life characterised by seclusion from the public and publicity.[334] 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.[335] In *Bernstein v Bester,*[336] Ackermann J held that the law recognises a very high level of protection of the individual's intimate personal sphere of life.

---

[329] A F Westin "Privacy and Freedom" (1967) 25(1) *Washington and Lee Law Review* 166.
[330] Snail *Cyberlaw @SA III: The Law of Internet in South Africa* 276.
[331] Neethling *et al Neethling's Law of Personality* 31.
[332] *R v Umfaan* 1908 TS 62.
[333] *R v Umfaan* 1908 TS 62 para 66 to 67, N Shaik-Peremanov "Basel II - The Right to Privacy: A South African Perspective" (2009) 21 *South African Mercantile Law Journal* 546 at 549 and J Church, C Schulze and H Strydom *Human Rights from an International and Comparative Law Perspective* 6th Edition (2007)196 to 201 and 225 to 268).
[334] Snail *Cyberlaw @SA III: The Law of Internet in South Africa* 277, C Okpaluba "Constitutional Protection of the Right to Privacy: The Contribution of Chief Justice (CJ) Langa to the Law of Search and Seizure" (2015) *ACTA JURIDICA* 407 at 408 and Neethling 2005 *South African Law Journal* 32.
[335] *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 271, *Jooste v National Media Ltd* 1994 (2) SA 634 (C) 645, *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T) 384, *Swanepoel v Minister van Veiligheid en Sekuriteit* 1999 (4) SA 549 (T) 553, *Motor Industry Fund Administrators (Pty) Ltd v Janit* 1994 (3) SA 56 (W) para 60, *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A) 462, *Bernstein v Bester* 1996 (2) SA 751 (CC) 789 and I M Rautenbach "The Conduct and Interests Protected by the Right to Privacy in Section 14 of the Constitution" (2001) *TSAR* 116.
[336] 1996 (2) SA 751 (CC) para 77.

The right to privacy recognises that every legal personality is entitled to a sphere of personal autonomy in which the law may not interfere. In *Financial Mail (Pty) Ltd v Sage Holdings Ltd*.[337] The Court held that the unlawful infringement of privacy is punishable in light of contemporary *boni mores* and the general sense of justice of the community as perceived by the Court. Since a person determines the destiny of his private facts and therefore, the scope of his interest is privacy. This power or competence of self-determination is considered the essence of a person's privacy and, therefore, his right to privacy.[338]

In *Bernstein v Bester,*[339] Ackermann J took a more limited view of privacy. According to him, privacy relates only to the inner sanctum of a person or his truly personal realm, such as his family life, sexual preference and home environment. [340] That is the most personal aspect of a person's existence and not every aspect within his knowledge and experience.[341] Therefore, privacy is infringed if others become acquainted with such information or disclose it to outsiders.[342]

The concept of privacy is too narrow since it negates other private facts relating to a person worthy of protection.[343] This applies particularly to the whole area of data protection. [344] The information processed about a person is often not of a most personal nature, or some of the data, taken on their own, are not even private according to the above description of privacy.[345] The total picture thereof is usually of

[337] 1993 (2) SA 451 (A) 462 to 463.
[338] *National Media Ltd v Jooste* 271 to 272 and J Neethling "Features of the Protection of Personal Information Bill, 2009 and the Law of Delict" (2012) 75 *THRHR* 241 at 244.
[339] 788, 789 and 795, J Neethling *et al Law of Delict* 7th Edition (2014) 347.
[340] Neethling 2005 *South African Law Journal* 20 and *Financial Mail (Pty) Ltd & Others v Sage Holdings* 462 to 463 and *Bernstein v Bester* 788, 789 and 795.
[341] Neethling 2005 *South African Law Journal* 20 and *Financial Mail (Pty) Ltd & Others v Sage Holdings* 462 to 463 (The Court held that the unlawfulness of an infringement of privacy is judged in light of contemporary *boni mores* and the general sense of justice of the community as perceived by the Court) and The Constitutional Court in *Bernstein v Bester* 788, 789 and 795 later endorsed this recognition and held that the right to privacy "relates only to the most personal aspects of a person's existence, and not to every aspect within his or her personal knowledge and experience."
[342] Neethling *et al Neethling's Law of Personality* 270 to 271, Neethling *et al Neethling on Personality Rights* 369 and Snail *Cyberlaw @SA III: The Law of Internet in South Africa* 291.
[343] Rautenbach 2001 *TSAR* 117.
[344] *Ibid*.
[345] *Ibid*.

such a nature that the person concerned determines the destiny of the data to be private and therefore also has the will to keep them private.[346]

In the case of *O'Keeffe v Argus Printing and Publishing Company Ltd*.[347] The plaintiff, a well-known radio personality, had consented to the publication of her photograph, being used for a newspaper article. The photograph was, however, used in the press for advertising purposes. Watermeyer AJ in the Cape Supreme Court consulted Voet's Commentary on *Digest*[348] for guidance and found examples of what could be classified as invasions of privacy (or *iniuriae*).[349]

The courts over the years also recognised unreasonable intrusions into the private sphere as actionable such as reading private documents,[350] bugging a person's room,[351] listening to private telephone conversations;[352] spying on someone while they are undressing.[353] All these are protected personality rights actionable under the common law of delict and the Constitution. The courts recognised certain unreasonable intrusions into the infringement of privacy as being sufficiently serious to warrant liability for criminal invasion of privacy in the form of *crimen iniuria*.[354]

---

[346] Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 545 and *Hyundai Motor Distributors (Pty) Ltd v Smit NO* 2001 (1) SA 545 (CC) para 557 Judge Langa DP held that "…The right to privacy does not relate solely to the individual within his intimate space, but is also retained in the social capacities in which people act for example when they are in their offices, in their cars or on mobile telephones…" and I Currie and J de Waal *The Bill of Rights Handbook* 6th Edition (2013) 302 to 303.

[347] 1954 (3) SA 244 (C).

[348] I Justinian *The Digest of the Roman Law: Theft, Rapine, Damage and Insult* Reprint Edition (1979) 47.10 (The digest was codified by Justinian I and published in A.D. 533).

[349] Watermeyer AJ acknowledged, however, that some of the examples referred to by Voet (such as the abduction of a matron's attendant and so exposing the matron to the degradation of being seen unattended) would hardly be regarded in more modern times as invading privacy.

[350] *Reid-Daly v Hickman* 1981 (2) SA 315 (ZA) 323.

[351] *S v A* 1971 (2) SA 293 (T).

[352] *Financial Mail Pty Ltd v Sage Holdings* 1993 (2) SA 451 (A).

[353] *R v Holliday* 1927 CPD 395 and *MEC for Health, Mpumalanga v M Net* 2002 (6) SA 714 (T) 718 to 719 and 721.

[354] *Huey Extreme Club v Mc Donald t/a Sport Helicopters* 2005 (1) SA 485 (C) 498 to 499. Some jurisdictions (such as the United Kingdom in 1997) have opted for anti-harassment or anti-stalking legislation (often providing for criminal penalties). However, in South Africa, the developed civil action for invasion of privacy and impairment of dignity (as well as the crime of *crimen iniuria*) provide adequate and preferable remedies against harassment and stalking.

Over the years since *the O'Keeffe* case was decided, the Supreme Court of Appeal has recently affirmed in *Grütter v Lombard*[355] the right to personal privacy, including a person's likeness and name. Endorsing the statement of O'Regan J in the Constitutional Court (CC) in *Khumalo v Holomisa*.[356] The Court believed that no sharp lines can be drawn between various facets of personality rights in giving effect to the value of human dignity in the Constitution. Nugent JA in *Grütter v Lombard*[357] concluded that the right to identity, subject to any defences based on legal policy, is protected under the South African law of privacy. Over the years, the remedy for invasion of privacy in South Africa has even been extended to protect a *juristic* person's right to privacy as well.[358]

3.2.1 Legitimate expectation of privacy

By providing personal information to the responsible party for a variety of reasons, such as credit applications and posting pictures online using cloud computing services, data subjects may be diminishing their own or minors' reasonable expectation of privacy.[359] These are decisions that could seriously impact the data subjects' and the child's right to privacy. Diminishing the right to privacy in this way may in future have a negative effect on the remedies available to them. In terms of the common law, the expectation will be that; their personal information is protected against all the possible risks of data breaches.

The legitimate expectation of privacy in the South African context has two components, namely, (a) a subjective expectation of privacy; (b) that is objectively

[355] 2007 (2) RSA (SCA) para 8 to 13.

[356] 2002 (5) SA 401 (CC) para 27; The Court stated that "…Drawing sharp lines between facets of personality can only serve to constrict the ultimate meaning of both privacy and dignity and deny the practical reality that 'personality' often defies compartments".

[357] 2007 (2) RSA (SCA) Para 13.

[358] *Financial Mail (Pty) Ltd v Sage Holdings Ltd* and *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 (4) SA 293 (A), Section 8(4) of the Constitution, which reads that: "A juristic person is entitled to the rights in the Bill of Rights to the extent required by the nature of the rights and the nature of the juristic person". "There is some authority that because juristic persons are not bearers of human dignity, their privacy rights may be attenuated" and *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others; In re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2001 (1) SA 545 (CC) para 18.

[359] P Gabriel "The Protection of Personal Information Act 4 of 2013 and Children's Right to Privacy in the Context of Social Media" (2019) 82 *THRHR* 605 at 611.

reasonable.[360] In determining whether a party has lost their legitimate expectation of privacy, a court will consider factors such as exposure to the public sphere and voluntary consent.[361]

There will be no expectation of privacy if one has voluntarily consented explicitly or implicitly to having one's privacy invaded. [362] The expectation of privacy will depend on how a person operates in the private or in the public sphere.[363] For example, when a data subject or a parent consents for and on behalf of their children to use their personal information on the Internet, they are thus potentially diminishing their and the children's legitimate expectation of privacy. Arguably, often without being fully informed about the nature, extent and repercussions of their actions.

While an individual may waive the right to exercise a fundamental right. The undertaking must be made clearly, freely and without the data subject being placed under duress or labouring under a misapprehension. [364] The decision whether, reasonably speaking, a person has a legitimate expectation of privacy may depend at least partly on whether the interference was of the "inner sanctum" of personhood or not, as the Constitutional Court pointed out in *Bernstein v Bester*.[365]

To be enforceable, the waiver has to be one of fully informed consent. It should clearly show that the person was aware of the exact nature and extent of the rights being waived in consequence of such consent.[366] Protecting this private and intimate sphere

---

[360] D Brand *et al South African Constitutional Law in Context* (2014) 463, *Snail Cyberlaw @SA III: The Law of Internet in South Africa* 277 to 278, Neethling *et al Neethling on Personality Rights* 372 and *Bernstein v Bester* para 75.

[361] *Bernstein v Bester* para 75.

[362] De Waal *The Bill of Rights Handbook* 298, Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 556, Neethling *et al Neethling's Law of Personality* 31 and Snail *Cyberlaw @SA III: The Law of Internet in South Africa* 278.

[363] I M Rautenbach *Bill of Rights Compendium* (1996) lA to178.

[364] Neethling *et al Neethling's Law of Personality* 31 and Snail *Cyberlaw @SA III: The Law of Internet in South Africa* 278.

[365] *Bernstein v Bester* para 2 and D Brand *et al South African Constitutional Law in Context* 463.

[366] *Mohamed and Another v President of the Republic of South Africa and Others (Society for the Abolition of the Death Penalty in South Africa and Another Intervening)* 2001 (3) SA 893 (CC) para 62.

provides the platform to establish and nurture human relationships without interference from the outside community.[367]

Bernstein v Betser was a follow up to *Ferreira v Levin*[368] and *Vryenhoek v Powell*[369] challenging, in part, searches and seizures of people involved in the winding down of a company. The Court stated that the scope of a person's privacy extends *a fortiori* only to those aspects in regard to which a legitimate expectation of privacy can be harboured. Ackermann J described what can be seen as a series of concentric circles ranging from the core most protected realms of privacy to the outer rings that would yield more readily to the rights of other citizens and the public interest.

As the legitimate right to privacy also extends to juristic persons,[370] however, the Constitutional Court found in *Investigating Directorate: Serious Economic Ofences v Hyundai Motor Distributors (Pty) Ltd In re: Hyundai Motor Distributors (Pty) Ltd v Smit*[371] that the privacy rights of a juristic person would be less intense than those of human beings. Although juristic persons like big companies and institutions also enjoy privacy protection, this protection would be weaker than for an ordinary human being.

3.3 The right to privacy in the context of cloud computing

The use of cloud computing has completely redefined communication techniques and the way of life with specific reference to the processing of personal information.[372] From mere sending of electronic messages and inquisitive web surfing, the Internet has come a long way with businesses being set up online to meet diverse consumer

[367] Snail *Cyberlaw @SA III: The Law of Internet in South Africa* 277, Brand *et al South African Constitutional Law in Context* 462, *Bernstein v Bester* para 75 and *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 (CC) para 32.
[368] 1996 (1) SA 984 (CC) para 1 and 1996 (1) BCLR 1 (CC) para157.
[369] 1996 (1) BCLR 1 (CC).
[370] The right to privacy also applies to juristic persons; *Financial Mail (Pty) Ltd v Sage* Holdings Ltd 1993 (2) All SA 109 (A).
[371] BCLR 1079 2001 (1) SA 545 (CC).
[372] U Joshi "Online Privacy and Data Protection in India: A Legal Perspective" (2013) 7 *NUALS Law Journal* 95, H T M Nguyen "Cloud Cover: Privacy Protections and the Stored Communications Act in the Age of Cloud Computing" (2011) 86 *Notre Dame Law Review* 2189 at 2189 and Kuner 2009 *Computer law and Security Review* 317.

needs.[373] The data breaches that have been experienced in the past decades across the world has indicated that a world without data breaches is improbable.[374] Cloud computing users are ignorant of how they can address these issues independently. The *status quo* can thus result in significant individual economic and emotional harm.[375]

Processing personal information using cloud computing services allows users to access high-end services and technology without trading quality for mobility.[376] Privacy and personal data are now under constant threat.[377] The personal information processed on cloud computing services can easily be made accessible. Many data collection devices and other techniques are being utilised, such as cell phones and tablets, so processed personal information can be easily provisioned through cloud computing services. The intrusions into the private affairs of individuals are at a more significant stake, thus giving rise to concerns pertaining to breach of privacy and the misuse of personal information.[378]

---

[373] Joshi 2013 *NUALS Law Journal* 95 and L Swales "Protection of Personal Information: South Africa's Answer to the Global Phenomenon in the Context of Unsolicited Electronic Messages (Spam)" (2016) 28 *South Africa Mercantile Law Journal* 49.

[374] Eliminating all data breaches in the context of cloud computing is generally neither technologically feasible nor socially desirable. Technological limitations mean that breach-proof security measures are impractical; this point can be supported by T Gonen "Data Breach Prevention is Dead" (February 9 2015) *The Hill* http://thehill.com/blogs/congress-blog/technology/ 232041-data-breach-prevention-is-dead (Accessed 09 August 2020) (This blog focuses more on the discussion of technological limitations). Moreover, economic and policy realities mean that companies are unlikely to invest in unlimited security measures mainly to save cost. From the corporate perspective, it may be more economically efficient to bear the cost of a breach ex-post than to invest in the security required to prevent the breach ex-ante. R Telang further supports this point "Policy Framework for Data Breaches" (2015) 13 *IEEE Security and Privacy* 77 at 79. He states that companies unwilling to bear such risk may also choose not to engage in the activity at all, which would be an unfortunate outcome both for business development and for consumers left unable to enjoy such products and services) and A Solow-Niederman "Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches" (2017 to 2018) 127 *Yale Law Journal Fisher* 614 at 618.

[375] T Hsu "Data Breach Victims Talk of Initial Terror, Then Vigilance" (9 September 2017) *New York Times* http://www.nytimes.com/2o17/o9/o9/business/equifax-data-breach-identity-theft-victims.html (Accessed 09 August 2020).

[376] P M Schwartz "Property, Privacy, and Personal Data" (2004) 117 *Harvard Law Review* 2055 at 2064.

[377] Joshi 2013 *NUALS Law Journal* 96, P Lanois "Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy" (2010) 9 *North-western Journal of Technology and Intellectual Property* 29 at 43 and Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 13 (Data subjects are generally not aware that a particular computerised agency holds their data profile. Furthermore, they usually do not know the nature and substance of the information, its accuracy, or how it is being used) and Smith "Cloud Computing for Business and Society at the Brookings Institution".

[378] V Reding "Privacy Matters: Why the EU Needs New Personal Data Protection Rules" (30 November 2010) http://europa.eu/rapid/pressReleasesActiondo?reference=SPEECH/10/700 (Accessed 20 July 2020), K Gormley "One Hundred Years of Privacy" (1992) *Wisconsin Law Review* 1335 to 1337 and S Mutkoski "Cloud Computing, Regulatory Compliance, and Student Privacy: A Guide for School

A survey carried out by Fortify Software amongst IT professionals at the DEF CON 2010 Hacker conference,[379] revealed that nearly 96% of the respondents believed that hackers view cloud computing services as having "a silver lining".[380] This meant that the hackers had identified certain flaws in using cloud computing that could be used to perpetrate data breaches to benefit cybercriminals.

3.4 Data protection in South Africa

The SALRC[381] describes data protection as an asset of safeguarding a data subject's right to privacy.[382] Data protection provides legal protection to the data subject when the responsible party processes the data subject's personal information.[383] The object of data protection laws is to regulate the processing of personal information and provide remedies for any infringements of the information right to privacy.[384]

The processing of personal information by the responsible party using cloud computing services threatens a person's privacy.[385] Under South African law, this threat can be viewed in three ways:

(i) The processing of personal information creates a direct threat to an individual's privacy. Privacy includes all those personal facts that a person himself determines should be excluded from the public.

(ii) The right to privacy becomes infringed if the public becomes acquainted with such information.[386]

Administrators and Legal Counsel" (2014) 30 *John Marshall Journal of Information Technology and Privacy Law* 511 at 519.

379 Reding "Privacy Matters: Why the EU Needs New Personal Data Protection Rules".

380 Press Release "Fortify: Survey Reveals Vast Scale of Cloud Hacking - and the Need to Bolster Security to Counter the Problem" (2010) *Press Release, Fortify Software, DEF CON* 1 https://www.globalsecuritymag.fr/Fortify-DEF-CON-survey-reveals,20100824,19100.html (Accessed 20 July 2020).

381 SALRC Discussion Paper 109, Project 124 and Neethling *et al Neethling on Personality Rights* 372.

382 Snail *Cyberlaw @SA III: The Law of Internet in South Africa* 291 and Neethling *et al Neethling's Law of Personality* 270.

383 Snail *Cyberlaw @SA III: The Law of Internet in South Africa* 291 and Roos 2007 *South African Law Journal* 401.

384 Roos 2007 *South African Law Journal* 402, Van der Merwe *et al ICT Law* 368 and De Wall *The Bill of Rights Handbook* 303.

385 Neethling *et al Neethling's Law of Personality* 270 to 271 and Van der Merwe *et al ICT Law* 416.

386 Snail *Cyberlaw @SA III: The Law of Internet in South Africa* 291, Neethling *et al Neethling's Law of Personality* 270 to 271 and Van der Merwe *et al ICT Law* 416. Identity was further recognised for the first time in South Africa as an independent personality right in the case of *Universiteit van*

(iii) The acquisition and revelation of false and misleading information may lead to the infringement of the data subject's identity elements.[387]

The two interesting cases that dealt with the infringement of a person's right to privacy in the South African context were *Bernstein v Bester's case.*[388] It provided a landmark ruling on the definition of privacy and a clear context of what it entails. This was the first case on the right to privacy decided upon by the Constitutional Court after adopting the Constitution under democratic South Africa.

Even though it was decided before the democratic dispensation, the other case was the case of *O'Keeffe v Argus Printing and Publishing Co Ltd.*[389]*In casu,* the Court recognised privacy as an independent right of personality worthy of being protected. The Court was of the view that much must depend upon the circumstances of each particular case, the nature of the personal information, the personality of the plaintiff, their station in life, their previous habits with reference to publicity and the like.[390]

3.4.1 The South African legal framework in relation to data protection

In terms of privacy and data protection law, be it constitutional, private or criminal law should not ignore the individual nature of the different interests of personality.[391] In many cases, an invasion of privacy through unlawful processing of personal information is sufficient to protect the data subject against imminent data breaches.[392] This is particularly true regarding consumers who enter into credit dealings with the

Pretoria v Tommie Meyer Films (Edms) Bpk 1977 (4) SA 376 (T) 386 and by the Supreme Court of Appeal in *Grutter v Lombard*. The SCA held that a person's name as a feature of their right to identity constitutes an interest capable of legal protection. A person's interest in preserving their identity against unauthorised exploitation is encompassed by the concept of *dignitus,* which incorporates both identity and privacy. Therefore, infringement of these interests is considered *iniuriae* under the South African common law. And as such, covered in both liability and remedies by the law of delict.

[387] Snail *Cyberlaw @SA III: The Law of Internet in South Africa* 291 and Neethling *et al Neethling's Law of Personality* 270 to 271.

[388] *Bernstein v Bester* 788, 789 and 795, Neethling *at al Neethling's Law of Delict* 347.

[389] This case was dealt with before the enactment of the Constitution, and therefore the common law was applied to decide by the Court.

[390] 249.

[391] J Neethling "The Constitutional Court Gives the Green Light to the Common Law of Defamation" (2002) 119 *South African Law Journal* 700 at 707.

[392] Neethling 2002 *South African Law Journal* 707 and Neethling *et al Neethling on Personality Rights* 365.

private sector who use certain state facilities that normally require the processing of certain personal information.[393]

In South Africa, privacy is protected in terms of the common law and the Constitution.[394] However, several statutory data protection legal instruments have been adopted in the past decades.[395] This section of the study will focus on the common law and the constitutional protection of the right to privacy. Processing of personal information by the data controllers threatens personality[396] as Neethling states that this threat takes place in two ways. Firstly, the compilation and distribution of such personal information.[397] Secondly, the acquisition and disclosure of false and misleading personal information may lead to the infringement of one's identity.[398]

Data subjects and the responsible parties are faced with two competing interests in cloud computing. The first interest is allowing technology to find its level in the marketplace.[399] This interest demands minimal government interference to ensure that the laws and regulations are in place and at the same time put the interest of the country and the public first.

The second interest is that of the individual and the guarantee that, with the new forces at work, the individual will be protected and the interests of the state.[400] In the democracy driven countries like South Africa, the United Kingdom and Canada, to mention but a few, the emphasis is on protecting the individual.[401] In other forms of

---

[393] Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 30.
[394] Shaik-Peremanov 2009 *South African Mercantile Law Journal* 546.
[395] Such as The Promotion of Access to Information Act 2 of 2000, National Credit Act 34 of 2005 and The Electronic Communications Act 25 of 2002.
[396] Neethling *et al Neethling's Law of Personality* 270, and Neethling *et al Neethling on Personality Rights* 369.
[397] Neethling *et al Neethling on Personality Rights* 369 and A Naude and S Papadopoulos "Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light to the Recent International Developments Part 1" (2016) *THRHR* 51 at 53.
[398] Neethling *et al Neethling on Personality Rights* 369 and Naude 2016 *THRHR* 53 and *National Media Ltd v Jooste*.
[399] A D Mitchell and J Hepburn "Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer" (2017) 19 *Yale Journal of Law and Technology* 182 at 185 to 188 and T Riley "Privacy and Data Protection: An International Bibliography" (1986) 7 *Journal of Media Law and Practice* 77.
[400] Riley 1986 *Journal of Media Law and Practice* 77.
[401] Yav 2018 *ITJ* 19.

government like China and India, protecting the state's interests is paramount.[402] Either way, the second interest clashes with the first. Today's challenge is to find the balance between these competing interests and ensure that as much as economic activities are provided, the right to privacy is not violated.

In principle, the unlawful processing of personal information is *contra bonos mores* and *prima facie* wrongful and a violation of the right to privacy.[403] The breach of privacy raises constitutional concerns.[404] There has been a growing sense in recent decades that an instantiation of the privacy violation risks infringe the right to freedom of speech as well.[405] The effect comes in as disclosing personal information on the press, which is likely to be processed using cloud computing services is questioned.[406] Such disclosure by the media can be a cause of action, and the data subject would hold the defendant liable for the publication or dissemination of personal information.[407] This could permit private plaintiffs to prevent or remove the speech of others in ways that censor speech and are thus antithetical to constitutional values.[408]

3.5 The Common Law protection of the right to privacy

The South African common law is a mixture of Roman-Dutch and English common law, which adopts the monist approach to customary international law. The courts are required to ascertain, recognise, use and administer rules of customary international law without the need for proof of law as in the case of foreign law.[409] As part of common law, customary international law is subordinate to all forms of legislation in South

---

[402] *Ibid.*
[403] Neethling *et al Neethling's Law of Personality* 273 and Snail *Cyberlaw @SA III: The Law of Internet in South Africa* 276.
[404] I Currie and J de Waal *The Bill of Rights Handbook* 5th Edition (2005) 14.
[405] S M Gilles "Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy" (1995) 43 *Buffalo Law Review* 1 at 6 to 9.
[406] E Volokh "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You" (2000) 52 *Stanford Law Review* 1049.
[407] Neethling 2002 *South African Law Journal* 707.
[408] N M Richards "The Limits of Tort Privacy" (2011) 9 *Journal of Telecommunications and High Technology Law* 357 at 365 to 374.
[409] *South Atlantic Islands Development Corporation Ltd v. Buchan* 1971 (1) SA 234 (C) 238.

Africa.[410] As part of the common law, customary international law is given a constitutional endorsement by section 232 of the Constitution.[411]

At common law, the right to privacy is delineated as an independent personality right[412] that the courts consider part of the concept of *dignitas*.[413] The concept of *dignitas*, before South Africa's constitutional dispensation, privacy protection was entrenched by virtue of ancient common law rights.[414] This refers to the *actio iniuriarum*, which protected privacy by affording a general delictual remedy for wrongs to an individual's personality. South Africa's courts first accepted this in *O'Keeffe v Argus Printing and Publishing Co Ltd.*[415]

Actio iniuriarum supposedly provides a valuable and sufficiently broad basis for recognising and protecting separate rights of personality.[416] Therefore, a person's personality right to privacy under the common law is actionable under the *actio iniuriarum*.[417] The right to privacy was also recognised by implication in the South African case law in the 1950s[418] under the *actio iniuriarum*[419] in the case of *Jansen van Vuuren v Kruger.*[420] Harms JA stated that the *actio iniuriarum* protects a person's *dignitas* and *dignitas* embraces privacy.

---

[410] *Inter-Science Research and Development Services (Pty) Ltd v Republica Popular de Mocambique* 1980 (2) SA I 11(T) 124 and *Kaffraria Property Co (Pty) Ltd v Government of the Republic of Zambia* 1980 (2) SA 709 (E) 712 to 715.

[411] Section 232 reads: "Customary international law is law in the Republic unless it is inconsistent with the Constitution or an Act of Parliament".

[412] *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T) 383 to 384 and D J McQuoid Mason *The Law of Privacy in South Africa* (1978) Chapter 4.

[413] McQuoid Mason *The Law of Privacy in South Africa* chapter 4, Currie *et al The Bill of Rights Handbook* para 14.3 and Church *Human Rights from an International and Comparative Law Perspective* 196 to 201 and 225 to 268.

[414] *Heroldt v Wills* 2013 (2) SA 530 (GSJ) para 7.

[415] para 247H to 249E and Snail *Cyberlaw @SA III: The Law of Internet in South Africa* 276.

[416] J Neethling "Personality Rights: A Comparative Overview" (2005) 38 *Comparative and International Law Journal of South Africa* 210 at 212, 216 to 218 and Neethling *et al Neethling's Law of Personality* 14 to 15.

[417] McQuoid-Mason 1982 *Computer and International Law Journal of South Africa* 136 and *Heroldt v Wills* 2013 (2) SA 530 (GSJ) para 7.

[418] *Mhlongo v Bailey* 1958 (1) SA 885 (E).

[419] Roos 2012 *South African Law Journal* 377, *National Media Ltd v Jooste* 267 and McQuoid Mason *The Law of Privacy in South Africa* 86.

[420] 1993 (2) All SA 619 (A).

This was further adjudicated upon in the case of *S v Bailey*.[421] Furthermore, in the case of *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk.*[422] Invasion of privacy was regarded as an aspect of impairment of *dignitas* under the *actio iniuriarum*. It follows then that, for a common-law action to succeed, the plaintiff must prove the elements of the delict, as discussed below.

In most cases, invasion of privacy involves intrusions or publicity.[423] The identification and delimitation of protected personality interests are of the utmost importance for, inter alia, the law of delict.[424] A delict is defined as wrongful, culpable conduct that causes harm to another person.[425] The law of delict is part of private law, the purpose of which is to regulate the relations between individuals in a community.[426]

Law of delict increases the courts' or the legislature's ability to articulate, develop and apply principles of legal protection.[427] This approach assists the judicature in determining how privacy, for example, differs from what has already been recognised or refused recognition under established legal theory and which measures are necessary for its protection.[428] In terms of the common law, the right to privacy is limited by the rights of others and the public interest.[429] In *Financial Mail (Pty) Ltd v Sage Holdings Ltd,*[430] the Court held that the unlawful infringement of privacy is judged

[421] 1981 (4) SA 187 (W).
[422] 1979 (1) SA 441 A.
[423] McQuoid-Mason 1982 *Computer and International Law Journal of South Africa* 136 and *Heroldt v Wills* 2013 (2) SA 530 (GSJ) para 7.
[424] Neethling *et al Neethling's Law of Personality* 29 and 416 (A serious infringement of the right to privacy is also actionable under the criminal law as *crimen iniuria*) as mentioned in C R Snyman *Criminal Law* 6th Edition (2008) 453, 457 to 458.
[425] *Ibid,* Neethling *et al Neethling's Law of Delict* 1, Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 540, T Takahashi "Drones and Privacy" (2012) 14 (1) *Columbia Science and Technology Law Review* 72 at 83 to 84 and Marsh and McLennan Companies "Dawning of the Drones: The Evolving Risk of Unmanned Aerial Systems" (2015*)* http://www.bit.ly/2nXQQoO (Accessed 02 December 2020).
[426] S Huneberg "On Drones, New Risk and Insurance" (2017) *THRHR* 586 at 586 to 587.
[427] McQuoid-Mason 1982 *Computer and International Law Journal of South Africa* 136 and *Heroldt v Wills* 2013 (2) SA 530 (GSJ) para 7.
[428] H Gross "The Concept of Privacy" (1967) 42 *NYULR* 34 and J Neethling "Tort Law in South Africa - The Mixing of the General and the Particular" (2001) *The Contribution of Mixed Legal Systems to European Private Law* 81 at 86.
[429] D H Flaherty "On the Utility of Constitutional Rights to Privacy and Data Protection" (1991) 41 *Case Western Reserve Law Re*view 831 at 832.
[430] 462 to 463.

in light of contemporary *boni mores* and the general sense of justice of the community as perceived by the Court.[431]

3.5.1 Application of the common law on the right to privacy

Even before the coming into force of the South African Constitutions of 1993 and 1996, South Africa's common law traditionally provided a degree of protection for a right of privacy. Such protection is illustrated by the judgement in *Powell NO v Van der Merwe.*[432] An overview of the constitutional protection of privacy developed in important judgments including *Berstein v Bester, Mistry v Interim Medical and Dental Council of SA,*[433] and *Magajane v Chairperson, North West Gambling Board*[434] is provided. [435]

South African jurisprudence has experienced little difficulty recognising the right to privacy as an independent right of personality.[436] This affirms the fact that personal information is protected. In *S v A,*[437] the accused was found guilty of *crimen injuria* because they installed a wireless bugging device in the complainant's apartment and listened in on his communications. It was held that an invasion of individual privacy sets a *prima facie* impairment of his *dignitas*.

3.5.2 The common law data protection

To establish the common law liability for an infringement of a personality interest such as the right to privacy, the plaintiff would have to establish that (i) there is an impairment of privacy either by disclosure or intrusion, (ii)wrongfulness and (iii) intention.[438]

---

[431] Shaik-Peremanov 2009 *South African Mercantile Law Journal* 549.
[432] *Powell v Van der Merwe* 2005 (5) SA 62 (SCA).
[433] 1998 (4) SA 1127 (CC).
[434] 2006 (5) SA 250 (CC).
[435] Neethling *et al Neethling's Law of Personality* 217 to 220, and J Neethling *et al Netthling's Law of Delict* 5th Edition (2006) 322.
[436] *Ibid.*
[437] 1971 (2) SA 293 (T).
[438] Neethling *et al Neethling's Law of Personality* 33 and 221 and Snail *Cyberlaw @SA III: The Law of Internet in South Africa* 277.

In many cases, the common law of delict, an action for invasion of privacy is sufficient to protect an individual against intrusions and publicity. With the introduction of cloud computing services, the efficacy of the common law action has been threatened.[439] This is particularly so regarding cloud computing services users who enter into transactions that involve the processing of their personal information with different sectors. These sectors make use of cloud computing services to process such personal information. It currently remains to be seen whether the common law may be sufficient to protect data subjects from the infringement of their right to privacy, to the extent that their personal information is unlawfully processed using cloud computing services.[440]

Under the common law, the data subject who feels that a responsible party has made unlawful processing of their personal information may have an action for invasion of privacy[441] Where for instance, incorrect but non-defamatory personal information is disclosed about him, the claim will not stand. If the disclosure is defamatory, an action will lie for defamation.[442]

Claims for invasion of privacy or violation of the right to privacy may be met with the defence of qualified privilege.[443] For instance, the responsible party has a legitimate interest in processing such personal information to safeguard their business interests when extending credit to the data subject or the responsible party has a reciprocal duty to make disclosure or processing of personal information, for example, a credit bureau to a client, the defence of qualified privilege may succeed.[444]

The processing of such personal information itself must be made in a reasonable manner and must be relevant to the occasion.[445] For example, in the case of personal

[439] McQuoid-Mason 1982 *Computer and International Law Journal of South Africa* 136 (Data subjects are generally unaware that a particular computerised agency holds their data profile. Furthermore, they usually do not know the nature and substance of the information, its accuracy, or how it is being used.).
[440] Roos 2007 *SALJ* 423.
[441] McQuoid-Mason *The Law of Privacy in South Africa* 198 and McQuoid-Mason 1982 *Computer and International Law Journal of South Africa* 139.
[442] *Pickard v SA Trade Protection Society* 1905 (22) SC para 89.
[443] McQuoid Mason *The Law of Privacy in South Africa* 199 and 225.
[444] *Morar v Casajee* 1911 EDL 171, 180.
[445] *Faydene Shirt 5 Clothing Manufacturers (Pty) Ltd v Levy* 1966 (1) SA 26 (D) para 30.

information given by credit bureaux, the subject matter should be confined to what is relevant to a person's creditworthiness. Only the relevant personal information must be furnished to the cloud computing client and not beyond the scope of the information requested.[446] The defence of qualified privilege has not been upheld in cases where credit bureaux have sent out incorrect personal information to a number of subscribers, irrespective of their interest in the plaintiff's standing.[447]

Consequently, where a cloud computing service provider or the responsible party unlawfully processes the data subject's personal information, they may be liable for damages. Where, on the other hand, the disclosure is made in response to a request concerning a particular individual's personal information for purposes such as state security or based on court orders, the occasion is likely to be privileged.[448]

When the litigation resumes for violating the right to privacy based on the unlawful processing of personal information, courts must decide on a case-by-case basis. The courts will determine whether a claim for the infringement of the right to privacy may succeed if the unlawful processing of personal information may not have been committed without using cloud computing to process such personal information.[449]

3.5.2.1 Elements of delict in the context of the right to privacy violation

The aggrieved data subject may enforce civil law delictual remedies against the responsible party.[450] To enforce a delictual claim successfully, the plaintiff has to prove that there was wrongful conduct, which was committed through fault on the defendant's part, and that it resulted in harm.[451]

For liability to be established and confirmed, the wrongdoer (the responsible party) must have committed intentional wrongful processing of personal information by

[446] E F Ryan "Privacy, Orthodoxy and Democracy" (1973) 51 *Canadian Bar* 84 at 88.
[447] *Ibid*.
[448] *Pickard v SA Trade Protection Society* 1905 (22) SC para 89.
[449] J Clarke "The Regulation of Civilian Drones' Impact on Behavioural Privacy" (2014) *Computer and Security Law Review* 287.
[450] Neethling *et al Neethling's Law of Personality* 221 and 292.
[451] *Ibid.*

invading the data subject's privacy using a cloud computing service.[452] Such an intention will be tested when a cloud computing platform has been used to process personal information, whether there was an intention to process such personal information unlawfully or not.[453]

The two most important requirements that need to be fulfilled to prove liability under the common law on data protection are wrongfulness and intent.[454] Furthermore, the data subject must be identified and linked to the personal information processed' if not, the processing of such personal information does not relate to the data subject.[455] Without the necessary proof, a factual infringement of the data subject's privacy would be lacking, and, consequently, wrongfulness would be absent.[456] In the cloud computing context, linking the data subject and the responsible party to the data breaches is a challenge as the information is stored on centralised servers elsewhere in the world.[457]

3.6 The protection of the right to privacy under the Constitution of South Africa

As a fundamental personality right deserving of protection as part of human dignity,[458] the right to privacy is entrenched in the Constitution. The constitutional concept of privacy is concerned with what can be described as informational privacy.[459] Section 14 of the Constitution provides that:

> "Everyone has a 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".

[452] *Ibid*.
[453] Roos 2007 *SALJ* 423.
[454] Neethling *et al Neethling's Law of Personality* 274.
[455] Neethling *et al Neethling's Law of Personality* 273.
[456] *Ibid* and *Misty v Interim Medical and Dental Association of South Africa* 1156.
[457] Narayanan 2012 *Chicago Journal of International Law* 785.
[458] Okpaluba 2015 *Acta Juridica* 407.
[459] *Bernstein v Bester* 792, *Protea Technology Ltd v Winer* 1997 (9) BLCR 1225 (W) 1241 and Van der Merwe *et al ICT Law* 417.

This section guarantees a general right to privacy, [460] with specific protection against searches and seizures and infringement of the privacy of communications. However, this list is not exhaustive. It extends to any other method of obtaining personal information, making unauthorised disclosures, or processing personal information.[461] The recognition and protection of the right to privacy as a fundamental human right in the Constitution indicate its importance.[462] The Constitution places immense value on the rights of the security of the human person and human dignity.[463]

Sachs J in *Mistry v Interim National Medical and Dental Council* stated the following:

> "…Generations of systematised and egregious violations of personal privacy established norms of disrespect for citizens that generally seeped into the public administration and promoted amongst a great many officials' habits and practices inconsistent with the standards of conduct now required by the Bill of Rights. The right to privacy accordingly requires us to repudiate the past practices that were repugnant to the new constitutional values, while at the same time re-affirming and building on those that were consistent with these values".[464]

The Constitution provides in section 38 that anyone acting in their interest or acting in the public's interest can approach a competent court, alleging that a right in the Bill of Rights has been infringed or threatened.[465] Then section 7(2) of the Constitution[466] creates a positive obligation on the state to "respect, protect, promote and fulfil" the rights in the Bill of Rights, including the right to privacy.

---

[460] Rautenbach 2001 *TSAR* 115, Currie *et al The Bill of Rights Handbook* 294, Brand *et al South African Constitutional Law in Context* chapter 12 and P De Vos "South African Constitutional Law in Context" (2014) *Research Gate* https://www.researchgate.net/publication/266031366 (Accessed 17 January 2021).

[461] *Ibid,* Van der Merwe *et al ICT Law* 416 and Currie *et al The Bill of Rights Handbook* 302 to 303.

[462] South African Law Reform Commission (2013) 40th Annual Report *Commonwealth Law Bulletin* 489.

[463] Neethling *et al Neethling's Law of Personality* 191, and M Laubscher and W J van Vollenhoven "Cyberbullying: Should Schools Chose between Safety and Privacy" (2015) 18 *Potchefstroom ELEC. L.J.* 2218 at 2235.

[464] *Mistry v Interim National Medical and Dental Council* 25.

[465] Section 38(a) reads; anyone acting in their interest and (d) reads anyone acting in the public interest and Currie *et al The Bill of Rights Handbook* 177 to 178.

[466] Which provides that the state must respect, protect, promote, and fulfil the Bill of Rights rights.

A court hearing the matter may grant appropriate relief and promote the values that underlie an open and democratic society based on human dignity, equality, and freedom.[467] However, suppose the court finds that there is the legislation regulating cloud computing in the context of the right to privacy, in that case, it will determine the matter based on such legislation first before considering the common law remedies.[468] Constitutional litigation may arise without legislative or common law remedies when a person claims that there has been a violation of their right to privacy based on the unlawful processing of their personal information using cloud computing services.[469]

The court in *Bernstein v Bester* held that caution must be exercised when attempting to project common law principles onto the interpretation of fundamental rights and their limitation. It was highlighted that it is important to keep in mind that, at common law, the determination of whether an invasion of privacy has taken place constitutes a single enquiry, including an assessment of its unlawfulness.[470] As in the case of other *iniuriae,* the presence of a ground of justification excludes the wrongfulness of an invasion of privacy. In constitutional adjudication under the Constitution, by contrast, a two-stage approach must be employed to decide a statute's constitutionality.[471]

As enshrined in section 14 of the Constitution, a breach of the right to privacy will be regarded as an unlawful invasion of privacy. Once the plaintiff has established her claim, the onus rests on the defendant to prove that the alleged breach was justified in terms of section 36. The plaintiff can also show that the invasion of privacy was justified in the circumstances. Fault is not a required element for a constitutional invasion of privacy.[472]

It then follows that the data subject has legitimate expectations regarding processing their personal information. In the case of *Mistry v Interim Medical and Dental*

[467] Section 38 read with section 39(1)(a), which must promote the values that underlie an open and democratic society based on human dignity, equality, and freedom.
[468] P De Vos and W Freedman *South African Constitutional Law in Context* (2015) 462.
[469] N Mashinini "The Processing of Personal Information Using Remotely Piloted Aircraft Systems in South Africa" (2020) 53 *De Jure Law Journal* 140 at 146.
[470] *Bernstein v Bester* para71.
[471] *Ibid*.
[472] D J McQuoid-Mason "Invasion of Privacy: Common Law v Constitutional Delict – Does It Make a Difference?" (2000) *Acta Juridica* 236.

Association of South Africa[473]*,* personal information was communicated by one medicine control inspector to another. The communication was for planning and implementing a search of the premises to carry out a regulatory inspection. It was argued that this was an invasion of privacy as protected by the then section 13 of the Interim Constitution.

It is clear that these instances of protection of the right to privacy correspond to the concept of privacy as a secluded condition of human life-embracing private facts. It does not constitute a numerous clause but may be expanded to any other obtaining or disclosing private information.[474] McQuoid-Mason observes that although section 14 of the Constitution creates a constitutional right to privacy, the supremacy of the Constitution does not mean that all previous notions of privacy will be forgotten and fall into disuse, such as the common law protection mechanisms[475] The same considerations that led to the entrenchment of a right to privacy in the Bill of Rights have long been recognised by the common law as important reasons for protecting the privacy and processing personal information. The degree of privacy that the citizen can reasonably expect may vary significantly, depending on the activity that brings them into contact with the state or the responsible party.[476]

Some legal commentators distinguish the constitutional right to privacy in section 14 into substantive and informational privacy rights.[477] The substantive privacy rights enable the data subject to make personal decisions about such interests with regard

---

[473] 1145.

[474] *Pretoria Portland Cement Co Ltd v Competition Commission* 2003 (2) SA 385 (SCA) 408 to 409 and 411, *Harksen v Lane NO* 1998 (1) SA 300 (CC) 331 to 332, *Klein v Attorney-General, Witwatersrand Local Division* 1995 (3) SA 848 (W) 865 (Restoring erased computer information), *Nel v Le Roux NO* 1996 (3) SA 562 (CC) 568 to 571, In the case of *NM v Smith* 2007 (5) SA 250 (CC) para 130, O'Regan Judge stated that "Although as human beings we live in a community and we are in a sense both constituted by and constitutive of that community. We are nevertheless entitled to a personal sphere from which we may exclude that community. We establish and foster intimate human relationships in that personal sphere and live our daily lives. The sphere in which to pursue our own ends and interests in our own ways although often mundane is intensely important to what makes human life meaningful".
and McQuoid-Mason 2000 *Acta Juridica* 249.

[475] S Woolman *et al Constitutional Law of South Africa* 2nd Edition (2008) 38 to 42 and Shaik-Peremanov 2009 *South African Mercantile Law Journal* 550.

[476] Shaik-Peremanov 2009 *South African Mercantile Law Journal* 550.

[477] Devenish *A Commentary on the South African Bill of Rights* 147.

to the processing of their personal information.[478] Informational privacy rights limit the ability of the responsible parties such as governments and companies to gain, publish, disclose or use personal information about others without their consent.[479] From this perspective, the constitutional right to privacy under section 14 is broader than the private law right since the former also includes autonomy.[480]

Although fiercely protected by jurisprudence in South Africa's Constitutional Court,[481] the right to privacy is not absolute and may be limited or infringed.[482] The limitations of this right can be justified in terms of section 36 of the Constitution.[483] The infringement or limitation is only lawful in terms of a law of general application. For example, an Act of parliament and the extent that the infringement or limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom.[484]

A person's right to privacy is always a balancing act[485] wherever the data subject is domiciled, this right must be balanced with and measured against other competing interests and rights such as freedom of speech, access to information and a state's right to national security. Each situation will turn on its facts. Suffice it to say that given South Africa's racial history, the right to privacy, although not absolute, is jealously protected. Recent legislative enactments and Constitutional Court judgments bear testimony to its value in South African society.

---

[478] *Curtis v Minister of Safety and Security* 1996 (3) SA 617 (CC) where Judge Didcott held that a ban imposed on the possession of erotic material "invades the personal privacy which section 13 of the interim Constitution ... guarantees that I shall enjoy".

[479] J Burchell "The Legal Protection of Privacy in South Africa: A Transplantable Hybrid" (2009) 13 *Electronic Journal of Comparative Law* 11 http://www.unuvu.eicl.oig (Accessed 10 August 2020).

[480] *Jooste v National Media Ltd* 645, *Bernstein v Bester* 789 and *Swanepoel v Minister van iligheid en Sekuriteit* 1999 (4) SA 549 (T) 553.

[481] *Khumalo v Holomisa* para 27.

[482] Swales 2016 *South African Mercantile Law Journal* 50 and C M van der Bank "The Right to Privacy-South African and Comparative Perspective" (2012) 1(6) *European Journal of Business and Social Sciences* 77 at 80.

[483] Section 36(1) of the Constitution is the limitations clause. In terms of the limitations clause, a general law of application may limit any right under the Bill of Rights if that limitation is justifiable and reasonable in an open and democratic society based on human dignity, equality and freedom. To test whether a limitation of constitutional rights is within the constitutional boundaries, the following factors and issues are considered: (a) the nature of the right; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; and the less restrictive means to achieve the purpose.

[484] Section 36 of the Constitution and *Khumalo v Holomisa* para 27.

[485] G E Devenish *The South African Constitution* 3rd Edition (2005) 86.

In the case of *the National Coalition for Gay and Lesbian Equality v Minister of Justice,* it became evident that South African jurisprudence in the area of privacy law is extensive. In this case, Justice Sachs explained that privacy recognises that every person has a right to a sphere of private intimacy and autonomy without interference from the outside community.[486]

In the case of *Le Roux v Direkteur Generaal van Handel en Nywerheid* [487] with regards to the processing of personal information. The court stated that the information held by the state in terms of the Interim Constitution 1993 section 23 on access to information, the court held that the information must be reasonably necessary for the exercise of the right. Section 23 of the Interim Constitution read that:

> "Every person shall have the right to access to all information held by the state or any of its organs at any level of the government in so far as such information is required for the exercise or protection of any of their rights".

For the processing of personal information to be deemed lawful, firstly, it must be certain that the protected interest is a legitimate one, recognised and protected by law.[488] Secondly, personal information may be used or communicated only to protect the legitimate interest involved.[489] Thirdly, it should be determined if the use of data is in a manner incompatible with the purpose for which it was requested.[490]

As discussed above, under the common law, the *actio iniuriarumn* is used to institute a delictual claim for infringement of privacy and unlawful processing of personal information.[491] However, constitutional principles must inform the application of the common law.[492] For legal action on infringement of privacy under section 14 of the

[486] *National Coalition for Gay and Lesbian Equality v Minister of Justice* para 32.
[487] 1997 (4) SA 174 (T) para 185.
[488] Neethling *et al Neethling's Law of Personality* 275.
[489] *Ibid.*
[490] *Ibid.*
[491] Roos 2012 *South African Law Journal* 396.
[492] *NM and Others v Smith and Others* 2007 (5) SA 250 (CC) para 28.

Constitution to succeed, the following must be proved: (a) impairment of the applicants' privacy; (b) wrongfulness; and (c) intention (*animius iniujriandi*).[493]

3.6.1 Invasion

A person should know of the existence of their personal information being processed by the responsible party.[494] This is regardless of how strong and comprehensive measures of protecting personal information are. It will be worthless if a data subject does not know the whereabouts of their personal information. Without such knowledge, the data subject's privacy will be threatened and even infringed.[495] The responsible party has a duty to notify the data subject concerning the processing of their personal information unless the data subject is already aware.[496]

For the individual to control their personal information, five elements must be fulfilled. Firstly, the data subject must be aware of the existence of a personal record or information concerning them stored at the responsible party's computers or premises.[497] Secondly, the data subject must be aware of the purpose or purposes for which their personal information was processed for.[498] Thirdly, the data subject must be legally entitled to access their processed information.[499] Fourthly, the data subject must be legally entitled to acquire the information about which persons have access to their personal information.[500] And lastly, the data subject is legally empowered to procure a correction or deletion of certain parts of the personal information.[501] For the traditional law remedies to be more effective, it appears that the data subject must be given active control over their personal information to be properly protected by law.

It can be argued that under the common law, the envisioned cause of action would be available when one party (the responsible party) has a legal duty to refrain from

---

[493] Neethling *et al Neethling's Law of Personality* 33.
[494] Neethling *et al Neethling's Law of Personality* 278.
[495] McQuoid Mason *The Law of Privacy in South Africa* 198.
[496] South African Law Reform Commission *Privacy and Data Protection* 168 to 171 and Neethling *et al Neethling's Law of Personality* 279.
[497] Roos 2006 *CILSA* 497 to 510 and South African Law Reform Commission *Privacy and Data Protection* 168 to 171 and 186 to 192
[498] *Ibid*.
[499] *Ibid*.
[500] *Ibid*.
[501] *Ibid*.

disclosing or processing personal information provided to it by another party (the consumer or data subject) beyond the scope of which it was processed. Furthermore, the responsible party has a legal obligation to provide and guarantee adequate protection of personal information processed by it.

The invasion of privacy as an impairment of *dignitas* under the *actio iniuriarum*,[502] distinguishes between two instances when privacy may be infringed in terms of the limitation of rights doctrine. Firstly, these two instances are the unauthorised acquaintance of personal information and the disclosure of such personal information. Secondly there must be an implicit or explicit confidentiality guarantee between the data subject and the responsible party.[503]

Other forms of infringements of the right to privacy include disclosing private facts acquired through unlawful intrusions, such as processing personal information unlawfully.[504] Publishing someone's photograph using cloud computing platforms without their consent is also an infringement of one's right to privacy.[505] The scenarios given above are certain forms of infringement that can also be perpetrated using cloud computing services. For instance, an unknown third party can hack the cloud computing server of the service provider to download certain information desired by them without them having to be physically present in a specific jurisdiction where the server is located or where the responsible party is located or even where the data subject is located.[506]

The disclosure of personal information for commercial purposes might lead the original, responsible party to share such information with a third party to complete the transaction. That would entail that the data subject trusted the third party to maintain such personal information securely as part of the chain of commerce. Should a data breach occur, the data subject's confidence would also be violated if the third party is

[502] *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* and *State v Bailey* 1981 (4) SA 187 (W).
[503] A B Vickery "Breach of Confidence: An Emerging Tort" (1982) 82(7) *Columbia Law Review* 1428 at 1456.
[504] *Epstein v Epstein* 1906 TH 87 para 88.
[505] *O'Keeffe v Argus Printing and Publishing Co Ltd* para 248H to 249A.
[506] Clarke 2014 *Computer and Security Law Review* 287.

breached.[507] In either instance, the argument under the common law is how the nature of the harm resulting from the responsible party's failure to secure personal information is distinct from the privacy violations on processing personal information using cloud computing platforms.

Responsible parties who use cloud computing services rely on the provider's assurance that the processed information will be adequately protected. Should a data breach occur on the servers of the cloud computing service provider, it can be presumed that the responsible party is not liable. However, the responsible party remains liable for damages in terms of the common law.

Where the elements of delict are met, a court may impose liability for breach of trust and invasion of privacy on the processing of personal information shared by the data subject as a breach of the right to privacy. This framework is based on the belief that when a data subject discloses personal information to the responsible party, they trust it will remain secure.[508]

This section further argues that responsible parties could be classified as what Jack Balkin calls "information fiduciaries".[509] Balkin presents information fiduciaries as a class of entities with trust with the data subjects. They are authorised to hold something valuable: personal information on behalf of that beneficiary.[510] Given this relationship of trust, such entities should properly be understood as possessing special duties to act in ways that do not harm the interests of the people whose personal information they process.[511] Balkin further suggests that information fiduciaries could have duties that differ from traditional fiduciaries.[512]

---

[507] Solow-Niederman 2017 to 2018 *Yale Law Journal Fisher* 622.

[508] J Litman "Information Privacy/Information Property" (2000) 52 *Stanford Law Review* 1283 at 1307 to 1308 and M Balkin "Information Fiduciaries and the First Amendment" (2016) 49 *University California Davis Law Review* 1183 at 1186.

[509] Balkin 2016 *University of California Davis Law Rev*iew 1186.

[510] *Ibid.*

[511] *Ibid* and J Zittrain "Response, Engineering an Election: Digital Gerrymandering Poses a Threat to Democracy" (2014) 127 *Harvard Law Review* 335 at 339 to 340.

[512] Balkin 2016 *University of California Davis Law Rev*iew 1186 and Zittrain 2014 *Harvard Law Review* 339 to 340 (Traditional fiduciaries are ordinarily individuals or entities that enter into a commitment to act in the best interests of a beneficiary. In designating a fiduciary, a beneficiary is entrusting a responsibility).

It is appropriate to tailor subcategories of information fiduciaries to fit different sorts of information sharing relationships under the common law in the context of the right to privacy.[513] This ideology suggests that responsible parties have a duty to securely process personal information that they receive from the data subjects. This envisioned confidential relationship does not arise from an explicit contractual agreement; it is instead emanating from an implied fiduciary relationship.[514] This fiduciary relationship may only develop after the data subject places trust and confidence in the responsible party's knowledge.[515]

If the data subjects did not voluntarily disclose their personal information by entering into a formal relationship with the breached entity,[516] then their right to privacy has been violated by that entity. If the responsible party knew it had their personal information yet made operational choices that failed to secure it, the responsible party would remain liable.[517] The proposed violation of breach of confidence can address and respond to these facts on the ground,[518] and would thus permit the common law to evolve to meet the challenges posed by cloud computing to process personal information.

3.6.2 Wrongfulness

The purpose of processing personal information must be lawful. Such purpose also determines the limits of lawful processing. The data subject must know the purpose. Suppose the data subject is unaware of what personal information is being processed and why, in that case, it becomes a challenge to judge whether processing that is taking place is lawful or not.[519]

---

[513] *Ibid*.
[514] W Hartzog "Reviving Implied Confidentiality" (2014) 89 *Indiana Law Journal* 763 at 770 to 772.
[515] Solow-Niederman 2017-2018 *Yale Law Journal Fisher* 626.
[516] B Fung "After the Equifax Breach, Here's How To Freeze Your Credit To Protect Your Identity" (9 September 2017) *Washington Post* http://www.washingtonpost.com/news/the-switch/wp/2o17/o9/o9/ (Accessed 10 August 2020).
[517] Vickery 1982 *Columbia Law Review* 1449 to 1451.
[518] *Ibid*.
[519] Neethling *et al Neethling's Law of Personality* 279.

In terms of the wrongfulness, if the personal information processed by the responsible party (defendant) is not adequately secure and an unauthorised person gains access to this information, injury occurs at that moment. This entails that the personal information is stolen; as soon as the responsible party's operational and systemic security decisions have allowed a breach to occur, wrongfulness would have occurred. The responsible party has violated the data subject's trust that any initial disclosure of personal information was limited to the particular context of the transaction with that distinct entity.[520]

Wrongfulness or an infringement of privacy is determined in accordance with the criterion of reasonableness or *boni mores.*[521] This is highlighted in the cases of *S v I*,[522] *S v A*[523] and *O'Keeffe v Argus Printing and Publishing Co Ltd.*[524] According to the positive law, wrongfulness could arise from infringing a subjective right (personality right) or the breach of a legal duty.[525] Apart from intrusion and disclosure, the mere unauthorised processing of personal information on cloud computing is also, in principle, wrongful.[526] Justification for wrongfulness includes the traditional grounds of justification such as necessity, self-defence, consent, and statutory or official capacity. The grounds of justification applicable in defamation cases, especially privilege and fair comment, should also justify an infringement of privacy.

Treating responsible parties as a form of a fiduciary is the key to invoking the common law principles in protecting the right to privacy under cloud computing. Fiduciary law relies on fact-bound analysis to identify implied as well as explicit relationships of trust between the data subject and the responsible party.[527] This assists in making its application appropriate when the data subject, as a condition of engaging in a transaction, would reasonably expect the responsible party to treat their personal

[520] J M Balkin "Information Fiduciaries in the Digital Age" (5 March 2014) *Balkinization* http://balkin.blogspot.com/2o14/o3/information-fiduciaries-in-digital-age.html (Accessed 09 August 2020) and Balkin 2016 *University California Davis Law Review* 1183.
[521] Neethling *et al Neethling's Law of Personality* 279.
[522] 1976 (1) SA 781 (A) 788 to 789.
[523] 1971 (2) SA 293.
[524] 248 and *National Media Ltd v Jooste* 2701 and *Gosschalk v Rossouw* 1966 (2) SA 476 (C) 492.
[525] Neethling *et al Neethling's Law of Personality* 279.
[526] Neethling *et al Neethling's Law of Personality* (2005) 231 236 and Gabriel 2019 *THRHR* 610.
[527] Hartzog 2014 *Indiana Law Journal* 771.

information securely.[528] To assess such wrongfulness will entail determining whether the data subject would have shared the personal information in question if they believed the data would not be secure. If the answer is "no", then it is reasonable to expect adequate protection of personal information. In addition, the guarantee of personal information security should extend to third-party actors associated with the responsible party.[529]

The acquaintance with private facts should thus be contrary to the subjective determination and will of the prejudiced party or data subject. At the same time, it should be viewed objectively and be unreasonable or contrary to the legal convictions of the community. This subjective-objective approach is similar to that of the Constitutional Court, which has held that the right to privacy will be protected. A person has a subjective expectation of privacy that society considers objectively reasonable.[530] The presence of a ground of justification will exclude the *prima facie* wrongfulness of an invasion of privacy. Such exclusion will apply if such limitation of the right to privacy is reasonable and justifiable in terms of the Bill of Rights section 36(1) of the Constitution.[531]

Whether an infringement of privacy will be regarded as wrongful will depend on society's *boni mores* or legal convictions, which requires an objective test based on

---

[528] Balkin 2016 *University California Davis Law Review* 1186 and Balkin "Information Fiduciaries in the Digital Age" (With the growth of the use of cloud computing in the global commercial sphere, one ironic consequence of the increase in data breaches may be that it appears less objectively reasonable for consumers to expect their data to remain secure. Yet the status quo of frequent breaches is not objective because it reflects a neutral state of play. Rather, it is equally likely to be a refraction of a system in which information and power asymmetries have led consumers to become resigned to the possibility of breaches, not because such frequent breaches are objectively reasonable in a nutshell. The envisioned cause of action would need to consider such dynamics in setting the appropriate initial benchmark for what represents a reasonable expectation. Furthermore, the proposed legal intervention is suggested as a start; over time, if it becomes clear that it is not reasonable for consumers to expect companies to keep their information secure, then it may be a signal that legislative or regulatory intervention strong enforcement mechanisms are, in fact, necessary to craft a sustainable solution as the widespread adoption of cloud computing as a form of processing personal information by many companies keeps growing regularly).

[529] Solow-Niederman 2017-2018 *Yale Law Journal Fisher* 629.

[530] Neethling 2004 *South African Law Journal* 520, *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit NO* 16 and *Bernstein v Bester* para 75.

[531] *S v Bailey* 1981 (4) SA 187 (N) 189, *Financial Mail (Pty) Ltd v Sage Holdings Ltd* para 462F to 463B, *National Media v Jooste* 270 and Neethling *et al Neethling's Law of Personality* 288.

the criterion of reasonableness.[532] The Constitutional Court considered public policy, public opinion, and society's *boni mores* in *Barkhuizen v Napier.*[533] The court held that public policy imports the notions of fairness, justice and reasonableness and denotes a general sense of justice of the community, the *boni mores,* manifested in public opinion.

It is submitted that, in principle, the mass publication of private facts is not reasonable; it goes against society's notions of fairness and should be considered to be *prima facie* wrongful.[534] This is so because such publication involves the processing of personal information. A proper example in terms of the processing of personal information unlawfully will be section 18(3)(c) of the Children's Act 38 of 2005 ("the Children's Act"). The Act provides that a parent or guardian of a child must give or refuse any consent required by law regarding the child.

Parents also have parental authority over their children in terms of the common law. In other words, where a parent consents to process certain personal information about their children, it is unclear whether this should be regarded as contrary to, or in line with, the *boni mores* of society.[535]

It is worth remembering that it was held in *S v Makwanyane*[536] that public opinion is no substitute for constitutional adjudication. The very reason for vesting the power of judicial review of all legislation in the courts is to protect the rights of minorities and others who cannot protect their rights adequately through the democratic process.[537] Arguably, normally ordinary citizens' data subjects are a class that cannot protect their rights adequately through the democratic process in the IT space and specifically against cloud computing service providers or users.

---

[532] *Steenkamp NO v Provincial Tender Board, Eastern Cape* 2007 (3) SA 121 (CC) and Gabriel 2019 *THRHR* 610.
[533] 2007 (5) SA 323 (CC) para 73.
[534] Neethling *et al Neethling's Law of Personality* 231 to 236.
[535] Gabriel 2019 *THRHR* 610.
[536] 1995 (3) SA 391 (CC) para 88.
[537] Gabriel 2019 *THRHR* 610.

Public policy, public opinion, and the *boni mores* of society thus should not necessarily be determinative.[538] Based on the mother-child example provided above. While society might feel that it is acceptable for a parent to consent for and on behalf of their child to process personal information on cloud computing platforms, such as the child's photographs on social media platforms.[539] The courts might determine that it is not in the child's best interests and that it should therefore be considered *prima facie* wrongful to do so.[540]

Assuming that, in bringing a delictual claim against the child's parents, a child can prove wrongfulness; the parent would be able to defend the claim by showing that the presence of consent excludes wrongfulness as a ground of justification. For such consent to be valid, the consenting person must have full knowledge of the extent of the possible harm and must appreciate the nature and extent of the infringement.[541] In the cloud computing context, most data subjects are ignorant about the data protection mechanisms used by cloud computing service providers.

Social media platforms such as Facebook and Instagram use cloud computing services to store a vast amount of personal information such as photographs and log-in details of an individual.[542] Arguably, many users or parents who consent for and on behalf of their children for their personal information to be published indiscriminately on social media platforms do so without full knowledge or consideration of the extent of the possible harm of their actions.

This raises concerns about whether such consent or ignorance should be considered valid for the responsible party to evade liability. Thus, the prospect of success of a delictual claim remains uncertain. First and foremost, it is unclear whether a data subject would successfully prove wrongfulness not. Secondly, the data subjects

---

[538] *Ibid*.
[539] *Ibid*.
[540] *Ibid*.
[541] *Hattingh v Roux NO and Others* 2011 (5) SA 135 (WCC) and Neethling *et al Neethling's Law of Delict* 111 to 113.
[542] J Q Anderson and L Rainie "The Future of Cloud Computing" (11 June 2010) *PEW Internet and American Life Project* http://pewresearch.org/pubs/1623/ future-cloud-computing-technology-experts (Accessed 25 July 2020).

themselves process their personal information on these social media platforms, making them both the data subject and the responsible party.

The element of wrongfulness, particularly under section 14 of the Constitution, is problematic and needs to be elaborated upon and clarified. Since the right to privacy in the context of processing personal information relates to personal details and facts that must remain private from an outsider (responsible party) who wants to process such personal information, the data subject should consent to it.[543]

It, therefore, follows that privacy can only be infringed if someone learns of true private facts about the person against their determination and will. Such knowledge can be acquired in one of two ways.[544] Firstly, through an intrusion, such as where the responsible party becomes acquainted with the facts,[545] or secondly, through a disclosure, such as where the responsible party reveals personal information that, although known to them, remains private to third parties.[546]

In considering when an infringement should be considered unlawful. One should distinguish between a situation where a data subject has made private facts known to a limited number of persons and where they have made the information known to an indeterminate, but still limited, number of persons.[547] In the first scenario, where personal information is made known only to a limited number of persons, the disclosure is characterised by an element of confidentiality. A responsible party's acquaintance with this information would be *prima facie* unreasonable and thus wrongful.[548]

Certain circumstances may make it apparent that the infringement should not be considered wrongful such as the limitation of rights as mentioned in section 36 of the

[543] *Hattingh v Roux NO and Others* 2011 (5) SA 135 (WCC) and Neethling *et al Neethling's Law of Delict* 111 to 113.
[544] McQuoid-Mason *The Law of Privacy in South Africa* 134 and G Hyman "The Concept of Privacy" (1967) 42 *New York University Law Review* 34 at 37.
[545] Roos 2012 *South African Law Journal* 396.
[546] *Ibid*.
[547] Neethling *et al Neethling's Law of Personality* 222.
[548] *NM v Smith* 44.

Constitution.[549] The Constitutional Court also made a similar observation in the case of *Mistry v Interim Medical and Dental Council of South Africa*[550] concerning the right to informational privacy. The court took into account that the data concerned had not been obtained in an intrusive manner but was volunteered by a member of the public.

In the second scenario, the acquaintance with the information by the responsible party will be *prima facie* reasonable. However, surrounding circumstances may reveal that it should be considered unreasonable and thus wrongful.[551]

The above scenario can be illustrated by referring to certain examples. If the data subject shares with the responsible party personal information in confidence, then a third party gets involved in the value chain in an unauthorised manner, such as hacking the server of the cloud computing service provider, the third party is infringing the right to privacy of the data subject. However, if the third party got involved by chance, both the data subject and the responsible party unknowingly carried out the processing of personal information and subconsciously or mistakenly involved the third party, the legal convictions of the community will not consider the third party's conduct to be unreasonable, and therefore, it will not be wrongful.

An example of the second scenario is where the data subject makes his personal information public, such as posting photographs on social media platforms that also use cloud computing services. Should someone use such publicised information without the data subject's consent, the data subject cannot claim that their right to privacy has been infringed since such information was already in the public domain. Anyone using such personal information would not be acting wrongfully since the information is in a public place.

---

[549] Limitation of rights 36 (1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including— (a) the nature of the right; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; and (e) less restrictive means to achieve the purpose. (2) Except as provided in subsection (1) or any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights, Neethling *et al Neethling's Law of Personality* 225 and Roos 2012 *South African Law Journal* 397.

[550] 1156.

[551] *Ibid*.

However, as Neethling argues and points out, that this does not mean that the processing of personal information available in public places can never be unreasonable.[552] For example, the processing of personal information without the data subject's consent is generally unlawful, contrary to the legal convictions of the community, and is, therefore, wrongful.[553]

The third type of situation that may arise is where a responsible party acquires the personal information of a data subject in accordance with the will and determination of the data subject. Then the responsible party discloses the personal information to a third party against the data subject's will. The wrongfulness of this disclosure is more challenging to determine. According to Neethling, such disclosure is not wrongful since sharing personal information with third parties in commercial transactions is inevitable. Such sharing of personal information normally forms part of the value chain to provide goods and services.[554] However, in certain circumstances, this conduct may be considered wrongful, for an example, if the shared personal information amounts to a mass publication of such information as an online advertisement from other parties that the data subject did not "contract" with, it would be considered unlawful and, therefore, wrongful.[555]

3.6.3 Intention

An essential requirement for liability under the *actio iniuriarum* is *animus iniuriandi* or intent. *Animus iniuriandi* is presumed once the wrongfulness of privacy infringement has been proven. The intention of a defendant is tested subjectively. A traditional negligence-based cause of action might seem more appropriate to avoid raising the duty of care so high as to make the cost of engaging in a socially desirable activity as the processing of personal information prohibitive.[556]

[552] Roos 2012 *South African Law Journal* 398.
[553] Neethling *et al Neethling's Law of Personality* 225.
[554] Neethling *et al Neethling's Law of Personality* 227.
[555] Neethling *et al Neethling's Law of Personality* 231.
[556] R Ahmed *The Explicit and Implicit Influence of Reasonableness on the Elements of Delictual Liability* (LLD Thesis, UNISA, 2018) 139 and Solow-Niederman 2017-2018 *Yale Law Journal Fisher* 630.

The two forms of fault recognised are intention (*dolus*) and negligence (*culpa* in the narrow sense).[557] In respect of the *actio legis Aquiliae* and the Germanic action for pain and suffering, fault in the form of intention or negligence is sufficient to ground delictual liability, provided that all the other elements are present. In respect to the *actio iniuriarum*, fault in the form of intention, *animus iniuriandi* (literally "the will to injure") is required.[558]

There are three forms of intent. A person can direct his will: directly (*dolus directus*) where the defendant desires to bring about a particular consequence. Indirectly (*dolus indirectus)*: The defendant desires to bring about a consequence but concurrently indirectly causes another consequence he is aware of. Thus, he has indirect intent in respect of the second consequence by actually subjectively foreseeing the possibility of a harmful consequence ensuing, reconciling himself with such possibility and nevertheless continuing with the conduct (*dolus eventualis*).[559]

The courts have applied the strict liability model for breach of confidence to establish liability.[560] Out of fairness to the responsible party, the proposed strict liability framework would be appropriate only in instances in which the plaintiff (data subject) can establish that the responsible party's conduct has failed to meet a well-instantiated security guideline or otherwise fallen below an established security standard.[561] This framework would not hold responsible parties liable, and some data breach victims would still be left without redress. If, for instance, a company complied with all known security standards and there was still a breach that affected the data subject, then that plaintiff would not be able to meet the requisite strict liability burden of proof.[562]

[557] Neethling *et al Neethling's Law of Delict* 130, R J Midgley and JC Van der Walt *Principles of Delict* 4th Edition (2016) 226 and M Loubser and R Midgley *The Law of Delict in South Africa* 3rd Edition (2018) 103.
[558] Loubser and Midgley *The law of Delict in South Africa* 103 to 104.
[559] *Black v Joffe* 2007 (3) SA 171 (C) 186, Midgley *Principles of Delict* 227 to 228, Loubser *The Law of Delict in South Africa Delict* 109 to 111 and Neethling *et al Neethling's Law of Delict* 133 to 135.
[560] Solow-Niederman 2017-2018 *Yale Law Journal Fisher* 629.
[561] Solow-Niederman 2017-2018 *Yale Law Journal Fisher* 631.
[562] However, this could entail that the plaintiff could not, for instance, claim that their password was stolen and offer as proof that the company failed to encrypt personal information, yet securely stored all password data and adequately encrypted.

If the courts could adopt and apply this formulation to data breaches in cloud computing services, what would change under this proposed strict liability formulation, is that a responsible party could no longer avoid liability if a data breach occurred. This would be based on the notion that if the responsible party did not implement adequate security standards or best practices and failed to protect the personal information, then the responsible party will be liable for the damages.[563] In a case where the plaintiff can provide such proof on a balance of probabilities and where the responsible party relationship is established, the injured party will be entitled to damages.

Shifting from negligence to a strict liability approach to address data breaches provides a way to seriously take the harm to the data subject when those reasonably expect to secure their personal information fail to do so. Firstly, even an informed and security-sensitive data subject may be unable to pursue effective self-help measures as far as data protection in cloud computing is concerned.[564] Secondly, the responsible party usually is better positioned to provide the steps that would bolster security for that entity in an efficient manner[565] as compared to the data subject. The data subject is unlikely to be privy to the responsible party's technological and operational practices.[566]

In the cloud computing context of data breaches, the strict liability approach can also be arguable problematic when the common law is applied. The argument and criticism of this approach could come in a scenario where a third-party hacker commits illicit actions that directly cause a data breach.[567] Under these circumstances, one could assume that the responsible party should not be held responsible for the third party's actions.

---

[563] Solow-Niederman 2017-2018 *Yale Law Journal Fisher* 632.

[564] J Coleman, S Hershovitz and G Mendlow "Theories of the Common Law of Tort" (2015) *Stanford Encyclopaedia of Philosophy* https://plato.stanford.edu/entries/tort-theories/ (Accessed 22 August 2020).

[565] *Ibid*.

[566] *Ibid*.

[567] H Marshall Jarrett *et al "*Prosecuting Computer Crime" (2010) *Office of Legal Education: Executive Office of U. S. Attorneys* 1 to 56 http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14 /ccmanual.pdf (Accessed 10 August 2020).

However, strict liability principles indicate why this intervening act should not necessarily eliminate the responsible party's liability.[568] In a scenario like this, strict liability applies if the responsible party processes personal information without implementing established security measures to protect data.

The strict liability approach is also applicable when third parties are involved in data breaches to holding the responsible party liable for the damage. An intervening act should not cut off liability if the responsible party's security measures increase the probability that the intervening act could occur or make the act possible in the first instance.[569]

The reasonableness of the defendant's conduct concerns lawfulness which is tested objectively. Although the common law does protect privacy to a degree, there is no common law principle that protects personal information *per se*. Therefore, it is comprehensible that specific legislation is required to address issues associated with personal information processing directly.

3.6.4 Reasonableness

Reasonableness is also a requirement under the common law data protection for the processing of personal information.[570] Reasonableness is part of natural law; it is based on the notion, not do to others that which you would not want them to do to you. [571] Natural law is given content by conclusions based on practical reasonableness.[572] Thus, natural law allows a person to infringe another's right under certain circumstances which may be justified and reasonable. For example, the infringement of the right to privacy for state security, the public's interest or court order.[573] The term "reasonableness" means: having sound judgement, fairness, the

[568] N A Sales "Regulating Cyber-Security" (2012) 107 *Northwestern University Law Review* 1503 at 1533 to 1539.
[569] D K Citron "Mainstreaming Privacy Torts" (2010) 98 *University of California Law Review* 1805 at 1836 to 1839.
[570] Neethling *et al Neethling's Law of Personality* 276.
[571] Ahmed *The Explicit and Implicit Influence of Reasonableness on the Elements of Delictual Liability* 11.
[572] *Ibid.*
[573] *Ibid*.

quality of being based on good sense, the quality of being appropriate or fair and moderateness.[574]

In South Africa, reasonableness has been linked to the concepts of justice, equality and fairness.[575] It is a vital component in relation to the protection of privacy in the cloud computing services context. Information obtained unlawful, such as private documents, is wrongful and unreasonable.[576] Suppose the processing of such information using cloud computing services is a continuation of wrongfulness under those circumstances. In that case, such personal information may not be processed because the processing is inseparably linked to the original wrongfulness, making such information processing unreasonable.[577]

If in the cloud computing context, such information was legitimated because it was a mere continuation of what is already in the system, then the industry will be tempted to use illegal means to process personal information.[578]

No more information than is necessary for the purpose it requested should be processed.[579] In the case of *Lex Roux v Direkteur-General van Handel en Nywerheid,*[580] the court held that the processing of personal information must be reasonably necessary. The same view was considered in the earlier case of *Gosschalk v Rossouw*.[581] Regardless of the certainty that the processing for the protection of legitimate interest must still be exercised reasonably.[582] The lack of reasonableness will invalidate the claim for damages.

[574]Ahmed *The Explicit and Implicit Influence of Reasonableness on the Elements of Delictual Liability* 19.
[575] *Ibid* and *S v Mokgethi* 1990 (1) SA 32 (A) para 40 to 41.
[576] Roos 2006 *CILSA* 281.
[577] Neethling *et al Neethling's Law of Personality* 277.
[578] *Ibid*.
[579] Neethling *et al Neethling's Law of Personality* 276.
[580] 185.
[581] 1966 (2) SA 476 (C) 490 to 492.
[582] Neethling *et al Neethling's Law of Personality* 122 and *Gosschalk V Rossouw* 1966 (4) SA 476 (C) 490 to 492.

It is also a reasonableness requirement that, upon request, the responsible party must allow the data subject concerned reasonable access to their personal information.[583] This access will provide certainty to the data subject whether the information is correct, necessary for the purpose and what kind of information is being processed. Furthermore, the data subject must be afforded the power to procure correction and deletion of misleading information or information processed unlawfully.[584] This right is essential for preventing or terminating an individual's personality interest infringement.[585]

3.7 Remedies for infringement of information privacy

If a person's right to privacy has indeed been infringed, then the remedies for such breach may be enforced through the *actio iniuriarum, the actio legis Aquiliae* or an interdict.[586] *The actio iniuriarum,* as discussed above, is used to claim satisfaction for the wrongful, intentional interference with the right to privacy. The *action legis Aquiliae* on the other hand, is used to claim patrimonial loss occasioned by the wrongful and negligent infringement upon privacy.[587]

An interdict is utilised when an imminent danger faces the person to prevent such an imminent intrusion. The person makes use of an interdict to avoid an ongoing wrongful infringement. The aggrieved party may obtain an interdict against the offender in such a case.[588] It is thus clear from the above that the common law has always protected the right to privacy, and so is the protection of personal information in particular.

3.7.1 Interdict as a data protection remedial mechanism

A data subject can apply for an interdict to prevent any responsible party or individual from unlawful processing or continuing to process personal information.[589] An interdict

[583] Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 505, South African Law Reform Commission *Privacy and Data Protection* 187 to 189 and Neethling *et al Neethling's Law of Personality* 279.
[584] Neethling *et al Neethling's Law of Personality* 279.
[585] Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 479 to 505 and Neethling *et al Neethling's Law of Personality* 279.
[586] Huneberg 2018 *THRHR* 265 and Neethling *et al Neethling's Law of Delict* 8 to 16 and 267.
[587] Neethling *et al Neethling's Law of Delict* 270 to 273.
[588] Neethling *et al Neethling's Law of Delict* 269.
[589] Van der Merwe *et al ICT Law* page 421.

may be final or temporary.[590] The requirements for the application of an interdict are (i) a clear right which is the right to privacy, (ii) an infringement to the right to privacy has materialised or reasonably apprehended to take place and (iii) the interdict should be the only available remedy.[591] A plaintiff may apply for an interdict and proceed with a separate damages claim.[592]

To obtain a final interdict, the plaintiff will have to prove that: - (i) they have a clear right, (ii) has suffered actual injury or has a reasonable apprehension of irreparable injury and (iii) no other satisfactory remedy is available.[593]For the application of an interdict, fault is not a requirement.[594] As much as the interdict can be a useful remedy for a data subject who wishes to stop the unlawful processing of personal information, it has its flaws.

In the case of cloud computing, personal information is available on the servers and various platforms in other jurisdictions. If an interdict is not issued before that information is processed, the long, expensive, and time-consuming litigation processes must be enforced. Suppose an interdict can be issued before the processing of personal information takes place. In that case, this will save costs, time and protracted expensive litigation processes and economic and emotional harm to the data subject. An interdict does not provide a clear understanding as to what extent can it be enforced against the responsible parties who are not domiciled in the South African territory and unlawfully process personal information.

3.8 The shortcomings of the common law and the Constitution

The traditional common law principles of protection of personal information could not adequately deal with the issues associated with cloud computing data breaches.[595] Section 14 of the Constitution further provided the constitutional protection of privacy

[590] Neethling *et al Neethling's Law of Delict* 269.
[591] Van der Merwe *et al ICT Law* page 421.
[592] *Rhodesian Printing and Publishing Co Ltd v Duggan and another* 1975 (2) All SA 125 (RA).
[593] McQuoid-Mason 2000 *Acta Juridica* 236.
[594] *Ibid*.
[595] Neethling *et al Neethling's Law of Personality* 289.

and enforcement of the protection of personal information.[596] Apart from the common law and the Constitution itself, there was a need for legislation that would deal specifically and fully with information protection; hence POPI Act was enacted.

It is my view that, since most cloud computing service providers are located in the US, the question that remains unanswered is on the application of the common law and section 14 of the Constitution on data breaches related to cloud computing. Firstly, the South African legal framework differs from that of the US. If the cloud computing service provider is based and incorporated in the US in terms of the company laws of the US complies with all the state's legal requirements, then that means the US law prevails.[597]

The injured party domiciled in South Africa could extend the jurisdiction in terms of the common law of delict against the responsible party based in the US; this will create a "conflict of laws". Secondly, often cloud computing services make a false sense of security as the users are not aware of where the data is processed and stored.[598] Nevertheless, access is available where the data is accessible once uploaded into storage in a fixed location such as a US-based cloud computing server. No contractual undertaking, for example, the Safe Harbour Framework, EU-USA Privacy Shield Framework or any other commission project or other business, will stop public law such as the Patriot Act of 2001 or the Foreign Intelligence Surveillance Act of 1978 from undermining any such an agreement.[599]

---

[596] The Preamble of the Protection of Personal Information Act and *Shabalala Msimang and Others v Sunday Times* 2008 (6) SA 102 (W) para 30 (In this case, the court stated that Shabalala Msimang enjoys the constitutional basis for her claim to the right to privacy which is protected by section 14 of the Constitution and must be allowed to enjoy it.).

[597] S Robert "Privacy, Technology and National Security, An Overview of Intelligence Collection" (2013) *Office of the Director on National Intelligence, Brookings Institution* https://www.dni.gov/index.php/ (Accessed 21 January 2021), The USA Patriot Act 2006: Preserving Life and Liberty, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (2003) *Department of Justice* https://www.justice.gov/ (Accessed 21 January 2021), The Foreign Intelligence Surveillance Act of 1978: Justice Information Sharing U.S. Department of Justice: *Office of Justice Programs Bureau of Justice Assistance* https://it.ojp.gov/ (Accessed 21 January 2021) and Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 32.

[598] Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 33.

[599] *Ibid.*

Voluntary disclosure can be prevented through contractual undertakings.[600] To succeed in a breach of contract suit based on prohibited voluntary disclosure, the claimant would have to find a way around the above mentioned legal indemnity. These indemnities include filing a claim against a foreign subsidiary based on foreign law.[601] Another often neglected fact is that the US cloud companies and their international divisions, particularly EU divisions are subject to the US disclosure regulations. These companies can be required to hand over data uploaded into storage anywhere in the world. If they do not follow such a request, they may face severe penalties.[602] What will then mean for the South African data subject under the current legal framework in the context of cloud computing data breaches to obtain legal remedy?

The common law has no explicit extraterritorial reach attached to it, which clearly outline and guarantee the remedial mechanisms and processes to be employed should a data breach occur in the cloud computing context outside the South African territorial borders. As a data subject, the common law does not explicitly mention where the personal information of the data subject is stored, how it should be processed, and the regulations in the event of a data breach.

The common law also places a burden on data subjects to be more active and on processing their personal information, which places a challenge in the cloud computing context. In cloud computing, it is a challenge for one to determine the destiny of their information, to whom it gets forwarded and how it is processed. The individual loses control of their information once such personal information is processed by the responsible party using cloud computing services.[603] A person's active control over his personal information can nevertheless be based on the recognition of the common law and the constitutional Court's decision in the case of *National Media Ltd v Jooste,*[604] and *Hyundai Motor Distributors (Pty) Ltd v Smit.*[605]

[600] *Ibid*.
[601] *Ibid.*
[602] *Ibid*.
[603] Van der Merwe *et al ICT Law* 367.
[604] 271 to 272.
[605] 2001 (1) SA 545 (CC) 557.

These judgments placed a burden on the data subjects to be more active and involved in how their personal information is processed. The court held that the right to privacy encompasses a person's competence to determine for himself the destiny of his private facts or the scope of his interest in his privacy.[606] Neethling and McQuoid-Mason raised a similar sentiment. They stated that an active control principle of the traditional protection principle is of little value if the data subject is not legally empowered to exercise direct control of their personal information.[607]

Finally, many countries, especially in EU, will require adequate international data protection in South Africa, which the common law does not provide, for the continued free cross-border flow of personal information through the use of cloud computing services.[608]

3.8.1 Challenges of the common law *actio iniuriarum*

One of the major hurdles on using the common law *actio iniuriarum* is that it is seldom used or never used against negligent conduct on processing personal information.[609] This is so because its main objective is to provide satisfaction or remedy for non-patrimonial loss caused by intentional and wrongful conduct.[610] Each case under the common law *actio iniuriarum* should be decided by the courts on a case-by-case basis. When the courts assess the infringement of a right to privacy claim, the facts and circumstances around such infringement determine the outcome. Should there be any, quantum to be awarded to the aggrieved data subject will be based on the courts' case-by-case assessment and approach criteria.

The court considers the plaintiff's social standing, such as an individual's intellectual capacity or position within the society or community. The impact of the violation of the right to privacy could cause based on the unlawfully processed information and the defendant's conduct, behaviour, and objective at the time and after the violation took

---

606 Neethling *et al Neethling's Law of personality* 273, Neethling 2005 *The Comparative and International Law Journal of Southern Africa* 233, *National Media v Jooste* 271 to 272 and *Hyundai Motor Distributors (Pty) Ltd v Smit* 557.
607 Neethling *et al Neethling's Law of personality* 278 and McQuoid Mason *The Law of Privacy in South Africa* 195.
608 Neethling 2012 *THRHR* 245.
609 Currie *et al The Bill of Rights Handbook* 297 and *NM v Smith* para 55.
610 *Ibid*.

place is also condidered.[611] The courts must further consider the negative effects on the plaintiff caused by the violation of their or its right to privacy.[612]

Based on the facts raised above, the common law *action iniuriarum* provides a more restricted approach in protecting data subjects' right to privacy on unlawful processing of personal information. The remedies it provides do not adequately protect data subjects from the negligent processing of personal information. This entails that this kind of protection does not meet the international standards required to protect personal information. It can, therefore, be raised as a concern that the cloud computing service providers, under the common law *action iniuriarum,* could evade liability for the infringement of the right to privacy of data subjects negligently.[613]

Any potential shortcomings in the protection afforded to aggrieved data subjects in terms of the common law may be mitigated if existing remedies are found to be adequate. However, it is submitted based on the above arguments that the existing remedies available to data subjects under the common law where their right to privacy has been infringed upon beyond reason are inadequate. Also, the threat to personality interests created by cloud computing services may require different remedies to those available in terms of the common law.[614] Lastly, the common law itself is subject to the Constitution and the legislation. Legislation has a more persuasive effect than the common law; therefore, there was a need for South Africa to adopt a specific data protection legislation.[615]

In another case of *Carmichele v Minister of Safety and Security.*[616] The court stated that there is a general obligation placed on the courts to develop the common law in

[611] Currie *et al The Bill of Rights Handbook* 297 and *NM v Smith* para 55 and Mashinini *De Jure Law Journal* 148.
[612] Currie *et al The Bill of Rights Handbook* 297.
[613] Mashinini *De Jure Law Journal* 149.
[614] Neethling *et al Neethling's Law of Personality* 281.
[615] *H v W* 2013 (2) All SA 218 (GSJ) para 31, The court held that: ("It is in respect of the remedy where infringements of privacy take place in the social media that the common law needs to develop … The law has to take into account changing realities not only technologically but also socially, or else it will lose credibility in the eyes of the people. Without credibility, the law loses legitimacy. If law loses legitimacy, it loses acceptance. If it loses acceptance, it loses obedience. The courts must respond appropriately to changing times, acting cautiously and with wisdom").
[616] *Carmichele v Minister of Safety and Security* 2001 (4) SA 938 (CC) para 39.

accordance with the spirit, objects and purport of the Bill of Rights.[617] Ackermann J and Goldstone J held that it needs to be stressed that the obligation of courts to develop the common law, in the context of section 39(2)[618] objectives are not purely discretionary.[619] On the contrary, it is implicit in section 39(2), read with section 173[620] that where the common law is deficient in promoting the section 39(2) objectives, the courts are under a general obligation to develop it appropriately.

They termed it a "general obligation" because they did not mean to suggest that a court must, in every case where the common law is involved, embark on an independent exercise as to determine whether the common law is in need of development and, if so, how it is to be developed under section 39(2). At the same time, there might be circumstances where a court is obliged to raise the matter on its own and require full argument from the parties.[621]

3.8.2 Shortcomings of the Constitution on the protection of the right to privacy

Constitutional litigation is expensive for aggrieved data subjects who cannot afford lawyers in South Africa.[622] Secondly, the burden lies with the plaintiff identifying the perpetrator who unlawfully processed their personal information, thereby infringing their privacy rights.[623] As mentioned in the previous chapter, data breach perpetrators can easily replace the IP address of the computer system so that the offence is presumed to come from a location other than the one from which it truly stems.[624] This

[617] South African Law Reform Commission *Privacy and Data Protection* 5.
[618] Section 39 (2) Interpretation of Bill of Rights: - When interpreting any legislation, and when developing the common law or customary law, every court, tribunal or forum must promote the spirit, purport and objects of the Bill of Rights.
[619] Neethling *et al Neethling on Personality Rights* 371.
[620] Section 173 Inherent power: - The Constitutional Court, the Supreme Court of Appeal and the High Court of South Africa each has the inherent ability to protect and regulate their process and to develop the common law, taking into account the interests of justice (Section 173 substituted by section 8 of the Constitution Seventeenth Amendment Act of 2012).
[621] *Carmichele v Minister of Safety and Security* 2001 (4) SA 938 (CC) para 39.
[622] C Fombad *Constitutional Adjudication in Africa* (2017) 170 and Mashinini *De Jure Law Journal* 146.
[623] Neethling *et al Neethling's Law of Personality* 273, Currie *et al The Bill of Rights Handbook* 298, Mashinini *De Jure Law Journal* 146 and *Misty v Interim Medical and Dental Association of South Africa* 1156.
[624] Rosenzweig *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* 78 and Lipson "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues" 14.

makes it difficult to trace the original computer or device where the data breach took place.

This makes it even more difficult for anyone to identify the perpetrator who conceals their identity using the wrong IP address. Such observations increase the burden on the aggrieved data subjects to enforce the right to privacy against violations committed through unlawful processing of personal information using cloud computing services. During the litigation processes, when the courts apply section 14 of the Constitution as contained in the Bill of Rights, the court must first consider the right to privacy by either applying enabling legislation or developing the common law to the extent that legislation does not give effect to that right.[625]

Secondly, it is further my view and argument that section 14 of the Constitution leaves a gap in protecting personal information. It does not explicitly provide remedies for the breach of personal information through cloud computing services. There are no outlined remedial mechanisms.

The Constitution is a domestic piece of legislation that has very limited influence or effect outside the territorial borders of a sovereign state unless supported by strong legislation that has extraterritorial reach. Section 14 only recognises the right to privacy as a fundamental human right in the Republic. Section 14 is vague and does not provide the detailed internationally required standard of data protection. Since the Constitution forms the cornerstone of democracy, it is in terms of section 14 that laid the foundation for the formation of the POPI Act.

[625] Section 8(3) reads that: When applying the provisions of The Bill of Rights to a natural or juristic person in terms of sub-section (2), a Court: –
(a) to give effect to the right in the Bill, must apply, or if necessary develop, the common law to the extent that legislation does not give effect to the right; and
(b) may develop the rule of the common law to limit the right, provided that the limitations are in accordance to section 36(1) and section 39(2) and (3) of the Constitution reads that: 39(2) when interpreting any legislation, and when developing the common law or customary law, every court, tribunal or forum must promote the and sub-section 39(3) reads: The Bill of Rights does not deny the existence of any other rights or freedoms that are recognised or conferred by common law, customary law or legislation, to the extent that they are consistent with the Bill.

Given the inherent conservatism of the courts. It is improbable**,** even if they fully comply with their general obligation to develop the common law in the light of the values underpinning the Bill of Rights,[626] that the application of the traditional principles in case law will occur often or extensively enough in the near future. Since the major engine for law reform should be the legislature and not the judiciary, the introduction of a data protection regime will involve incremental changes of the common law and radical law reform; which is a task for the legislature.

3.9 Conclusion

The overview of data privacy policies and regulations in South Africa indicates that its current state is well developed, however, there are prospects for continued growth to keep up with the international data protection standards. Adopting the statutory laws and regulations that would regulate cloud computing in South Africa is the best way to provide adequate data protection to its citizens and meet the international data protection requirements.

[626] Constitution section 39(2), *Carmichele v Minister of Safety and Security (Centre for Applied Legal Studies Intervening* 2001 (4) SA 938 (CC) para 953ff*, Van Eeden v Minister of Safety and Security (Women's Legal Centre Trust as* amicus curiae) 2003 (1) SA 389 (SCA) 395, *Minister of Safety and Security v Van Duivenboden* 2002 (6) SA 431 (SCA) 444, *Dendy v the University of the Witwatersrand, Johannesburg* 2005 (5) SA 357 (W) 371 to 372, Neethling *et al Neethling's Law of Delict* 17, Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 548 and 649 to 650 and Neethling 2012 *THRHR* 245.

Chapter 4: The influence of the Protection of Personal Information Act 4 of 2013 (POPI Act) on the regulation of privacy in the Cloud Computing context

4.1 Introduction

In general, the object of data protection laws is to regulate the processing of personal information.[627] The data protection laws aim to give legal protection to a person concerning the processing of personal information about themselves (data subject) by another person or institution (responsible party).[628] These legal frameworks have common characteristics, they contain a set of data protection principles that inter alia give the data subjects active control over the processing of their personal information while recognising and providing protection to the constitutional right to privacy.[629]

The POPI Act does not address cloud computing explicitly and exclusively as the only form of processing personal information. As discussed above, cloud computing involves cross-border data flows. The POPI Act aims to regulate the flow of personal information across the Republic's[630] borders and provide for matters connected therewith.[631]

This chapter aims to analyse selected provisions and specific terms used in the POPI Act in the context of cloud computing. It is impossible to provide a meaningful discussion of all the provisions of the POPI Act in the limited space and time on one research study. Since the chapter aims to determine whether the POPI Act provides "adequate" data protection, the discussion will focus on some of the provisions that are considered essential to attaining adequacy in a cloud computing context. The last

[627] A Roos "Privacy in the Facebook Era: A South African Legal Perspective" (2012) 129 *South African Law Journal* 375 at 379.
[628] Neethling *et al Neethling's Law of Personality* 267, and Roos 2012 *South African Law Journal* 379.
[629] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1981) Paris and The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention No 108/ 1981, Strasbourg 28 January 1981, which both have a set of principles of data protection. For example, the OECD Guidelines contain principles of personal information processing specifications. and A Roos "Core Principles of Data Protection Law" (2006) 39 *CILSA* 102 at 107.
[630] Section 1 of the Protection of Personal Information Act defines the term "Republic" as the Republic of South Africa.
[631] The Preamble of the Protection of Personal Information Act.

section will look at the other obstacles of the POPI Act on regulating the right to privacy and the concluding remarks of the chapter.

4.2 The purpose of the POPI Act

POPI Act's aims are first set out in its Preamble to promote and protect personal information processed by public and private bodies subject to justifiable limitations.[632] Such limitations aim to balance the right to privacy against other rights, particularly the right of access to information.[633] According to the Act's Preamble, section 2 read with section 3(1)(a) of the Act; the legislation aims to protect the right to privacy enshrined under section 14 of the Constitution.[634] The right to privacy includes protection against the unlawful collection, retention, dissemination and use of personal information.[635] The notion that information privacy is a sub-category of the right to privacy is echoed in the definition of "personal information" as contained in section 1 of the POPI Act.

Section 2(a)(ii) states that the Act aims to protect specific vital interests, including the Republic's free flow of personal information[636] and across international borders.[637] Section 2(b) establishes conditions for responsible parties' lawful processing of personal information.[638] These conditions should be in harmony with international standards that prescribe the minimum threshold requirements for the lawful processing of personal information.[639] The Act also provides data subjects with some control over

[632] The Preamble, sections 2, 3 and 72 of the Protection of Personal Information Act.
[633] Section 2(a)(i) of the Protection of Personal Information Act.
[634] The Preamble of the Protection of Personal Information Act and Neethling *et al Neethling on Personality Rights* 373.
[635] The Preamble of the Protection of Personal Information Act, Information Regulator of South Africa: Amended Notice Relating to Amended Guidelines to Develop Codes of Conduct in terms of Chapter 7 of the Protection of Personal Information Act of 2013 3 https://www.justice.gov.za/inforeg/docs/20181214-gg42110-rg10897-gon1383-POPIregister pdf (Accessed 02 March 2021) and Swales 2016 *South African Mercantile Law Journal* 49.
[636] Section 1 of the Protection of Personal Information Act defines the term "Republic" in terms of the Act as the Republic of South Africa.
[637] Section 2(a)(ii) of the Protection of Personal Information Act and Neethling *et al Neethling on Personality Rights* 373.
[638] Chapter 3 of the Protection of Personal Information Act and Neethling *et al Neethling on Personality Rights* 365.
[639] Neethling *et al Neethling on Personality Rights* 373 (The GDPR provides international data protection standards guidelines. It was adopted and put in force on 25 May 2018. When the POPI Act was drafted, the international data protection standards were provided for by the OECD guidelines on data protection and the EU Directives (which the GDPR later replaced).

their personal information.[640] The Act further provides data subjects with remedies to protect their personal information from processing that is not according to its provisions.[641] Moreover, the Act aims to establish voluntary and compulsory measures to protect the right to privacy.[642] These measures include the establishment of an Information Regulator (IR). The IR has to ensure respect for and promote, enforce and fulfil the rights protected by the POPI Act.[643]

POPI Act generally protects data subjects' personal information regardless of the medium used to process such personal information.[644] For POPI Act provisions to be applicable, personal information must be processed using automated or non-automated means.[645]

---

[640] Section 5 of the Protection of Personal Information Act outlines the rights of data subjects. It states that a data subject has the right to have his, her or its personal information processed under the conditions for the lawful processing of personal information as referred to in Chapter 3, including the right—
(*a*) to be notified that—
(i) personal information about him, her or it is being collected as provided for in terms of section 18; or
(ii) his, her or its personal information has been accessed or acquired by an unauthorized person as provided for in terms of section 22;
(*b*) to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information as provided for in terms of section 23;
(*c*) to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of section 24;
(*d*) to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information as provided for in terms of section 11 (3) (*a*);
(*e*) to object to the processing of his, her or its personal information—
(i) at any time for purposes of direct marketing in terms of section 11 (3) (*b*); or
(ii)in terms of section 69 (3) (*c*);
(*f*) not to have his, her or its personal information processed for purposes of direct marketing using unsolicited electronic communications except as referred to in section 69 (1);
(*g*) not to be subject, under certain circumstances, to a decision which is based solely on the automated processing of his, her or its personal information intended to provide a profile of such person as provided for in terms of section 71;
(*h*) to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in terms of section 74; and
(*i*) to institute civil proceedings regarding the alleged interference with protecting his, her or its personal information as provided for in section 99.

[641] Section 2(c) of the Protection of Personal Information Act.

[642] Section 2(d) of the Protection of Personal Information Act.

[643] *Ibid* and Neethling *et al Neethling on Personality Rights* 373.

[644] Section 1 of the Protection of Personal Information Act and Mashinini 2020 *De Jure Law Journal* 153.

[645] Section 3(1)(a) of the Protection of Personal Information Act.

It is paramount to understand the Act's scope to employ proper statutory interpretation theories and apply its provisions properly on a case-by-case basis. The POPI Act scope will be analysed in a cloud computing context in the following paragraphs.

4.3 The scope of the POPI Act

The scope of the POPI Act applies to responsible parties who are domiciled in the Republic or not domiciled in the Republic but makes use of automated or non-automated means in the Republic.[646] The Act does not apply to non-South African domiciled responsible parties who only use cloud computing services to forward personal information through the Republic.[647] However, if the processing involves activities of certain public institutions, such as those involved in combating terrorism, crime and money laundering, they are excluded from the Act.[648]

The POPI Act regulates the processing of personal information that forms part of a filing system or entered in a record to form part thereof.[649] The Act also provides the introduction of specific conditions to establish minimum requirements for personal information processing.[650] POPI Act further places an obligation to the State to respect, protect, promote, and fulfil the Bill of Rights (the right to privacy is included).[651]

---

[646] Section 3(1) of the Protection of Personal Information Act.

[647] Section 3(1)(b)(ii) of the Protection of Personal Information Act and Neethling *et al Neethling on Personality Rights* 373.

[648] Section 6(1)(c)(i) of the Protection of Personal Information Act.

[649] Section 2 of the Protection of Personal Information Act, Mashinini 2020 *De Jure Law Journal* 149 and Section 73 of the Protection of Personal Information Act which deals explicitly with interference with the protection of the personal information of a data subject and determines, among other things, that a breach of the conditions for the lawful processing of personal information will constitute a violation of a data subject's right to privacy. Failure to comply with the requirements of lawful processing as set out under Chapter 3 of the Protection of Personal Information Act will thus render the processing of personal information unlawful, thus providing the aggrieved data subject with a civil action for damages in terms of section 99 and as prescribed by section 5(1)(i) against a responsible party.

[650] Chapter 3 of the Protection of Personal Information Act and D Millard and E G Bascerano "Employers' Statutory Vicarious Liability in Terms of the Protection of Personal Information Act" (2016) 19 *Potchefstroom Electronic Law Journal* 1 at 3 and K Allan and Iain Currie "Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa" (2007) 23 *South African Journal on Human Rights* 570 at 573.

[651] The Preamble of the Protection of Personal Information Act and Guidance Note on the Processing of Personal Information in the Management and Containment of Covid-19 Pandemic in Terms of the Protection of Personal Information Act 4 of 2013 section 2(2) The Regulator is issuing this Guidance Note to- 2.2.1. give effect to the right to privacy as it relates to the protection of personal information; 2.2.2. guide the public and private bodies and their operators on the limitation of the right to privacy when processing personal information of data subjects to contain the spread and reduce the impact of COVID-19 https://www.justice.gov.za/ (Accessed 27 January 2021).

It further entails providing a balance of the constitutional values of democracy while allowing the free flow of personal information for economic and social activities in harmony with the international standards of data protection.[652]

The Act applies, subject to section 3(b), to exclude any other legislation that regulates the processing of personal information.[653] Such legislation should be materially inconsistent with an object, or a specific provision, of the POPI Act.[654] It must be noted that if any other legislation provides conditions for the lawful processing of personal information more extensive than those set out in Chapter 3 of the POPI Act, the extensive conditions prevail.[655] The scope of the POPI Act includes the application and interpretation provisions under section 3 to archive its purpose.

4.4 Application and interpretation of the POPI Act

The provisions of section 3 of the POPI Act deal with the Act's application and interpretation.[656] The Act applies to processing personal information entered in a record by or for a responsible party using automated means (cloud computing) or non-automated means.[657] If the processing takes place by non-automated means, the record must form part of a filing system or be intended to form part of such a system.[658] According to specific criteria, the Act will only apply to manually processed personal information if such information is readily available and accessible.[659]

In terms of the interpretation of the POPI Act, section 3(3) provides that the Act must be interpreted in a manner that gives effect to its purpose. The statutory interpretation

[652] The Preamble, sections 2, 3 and 72 of the Protection of Personal Information Act, South African Law Reform Commission *Privacy and Data Protection*, Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 477 to 479*,* A Roos "The European Union's General Data Protection Regulations (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'" (2020) 53(3) *Comparative and International Law Journal of Southern Africa* abstract*,* Neethling *et al Neethling's Law of Personality* 281 and Neethling 2012 *THRHR* 245.
[653] Section 3(2)(a) of the Protection of Personal Information Act.
[654] *Ibid*.
[655] Section 3(2)(b) of the Protection of Personal Information Act.
[656] The date of commencement of section 3 was 1 July 2020.
[657] Neethling *et al Neethling on Personality Rights* 373.
[658] Section 3(1)(a) of the Protection of Personal Information Act and Neethling *et al Neethling on Personality Rights* 373.
[659] *Ibid*.

of the Act should not prevent any public or private body from exercising or performing its powers, duties and functions in terms of the law and such powers, duties, and functions related to the processing of personal information. Such processing has to follow the Act or any other legislation, as referred to in subsection (2), that regulates personal information processing.[660]

The primary rule of statutory interpretation is to determine the legislature's intention by giving the words in the provision their ordinary grammatical meaning unless to do so would lead to absurdity that the legislature could not have contemplated. In the case of *Bato Star Fishing* (*Pty*) *Ltd v Minister of Environmental Affairs and Tourism*[661] in an undivided Constitutional Court per Ngcobo J, the Court identified itself with the emerging trend in statutory construction to regard the context in which the words occur, even where the words to be construed are clear and unambiguous.

The Court referred with approval to *Thoroughbred Breeders' Association v Price Waterhouse.*[662] The Court voiced concerns about an interpretive approach that pays too much attention to the words' ordinary language. The Court stated that it ignores the colour given to the language by the context. As per the Court's view, that context is the constitutional commitment to achieving equality. The foundational policy of the Act is to transform the industry consistent with the Constitution, and the Act read as a whole. A similar sentiment was also echoed in the case of *Ngweyama v Mayelane*.[663]

The POPI Act's interpretation and application must not be restricted to the explicitly addressed forms of personal information processing. The courts are obliged to preside over the unlawful processing of personal information on a case-by-case basis. Such an approach assists in realising the Act's scope, intention, and purpose of different sections and subsections.[664] Statutory interpretation theories must be considered to interpret a statute in everyday practice, and they can be considered separately from each other,[665] hence the title of section 3 entails the application and interpretation of

[660] Section 3(3)(b) of the Protection of Personal Information Act.
[661] 2004 4 SA 490 (CC) para 90.
[662] 2001 4 SA 551 (SCA) para 12.
[663] 2012 3 All SA 408 (SCA) 409.
[664] Section 3(a) of the Protection of Personal Information Act.
[665] E Steyn and A Nicol *Handbook of Trauma for Southern Africa* 5th Edition (2017) foreword viii to ix.

the POPI Act.[666] In this section, the interpretation of the POPI Act will be made in the context of cloud computing as a mechanism to process personal information and the right to privacy.

4.4.1 Brief background on the interpretation of the statute

Statutory interpretation is an interplay of human action and reasoning, and the theory of interpretation cannot accurately predict the outcome of interpretive endeavours.[667] Cross defines statutory interpretation as the process by which the courts determine the meaning of a statutory provision to apply it to the situation before them.[668] In this instance, different types and levels of reasoning of a person when reading a statute and applying them to each case being decided upon fall under what can be termed theories of interpretation. These theories will then proclaim some preferred *modus operandi* for interpreting statute without comprehensive, explanatory or justificatory models themselves.[669]

The conventional common law theories of statutory interpretation are mainly theories in such a restricted sense. The discussion in this chapter is; literalism, intentionalism, purposivism, Judicial activism and objectivism.[670] Definitions and discussion of these theories fall outside this research scope; some will be, however, be defined and explained briefly to clarify the argument raised. More than one of these theories at the same time may inform a broader theoretical position on an approach to or a particular trend in statutory interpretation.

---

[666] Section 3(a) of the Protection of Protection Information Act.

[667] L M du Plessis *An Introduction to Law* 3rd Edition (1999) 242 to 243. (as revised and published online by University of Cambridge Press 2008) The complexity of language impacts legal interpretation and G E Devenish *Interpretation of Statutes* (1992) 2.

[668] A Singh *The Impact of the Constitution on Transforming the Process of Statutory Interpretation in South Africa* (LLD Thesis, UKZN, 2014) 4 and R Cross *Statutory Interpretation* 3rd Edition (Revised) (1995) 40.

[669] Singh *The Impact of the Constitution on Transforming the Process of Statutory Interpretation in South Africa* 4.

[670] Devenish *Interpretation of Statute*s 25 to 56, Singh *The Impact of the Constitution on Transforming the Process of Statutory Interpretation in South Africa* 29, L M du Plessis "Theoretical (Dis-) position and Strategic Leitmotivs in Constitutional Interpretation in South Africa" (2015) 18(5) *Potchefstroom Electronic Law Journal* 1332 at 1335 and L M du Plessis *Re-Interpretation of Statutes* (2002) 89 to 119.

Theoretical positions that South African courts have displayed and theories of interpretation they have invoked in day-to-day practice will be considered to interpret the POPI Act in the context of cloud computing. The Interpretation Act[671] defines law as any law, proclamation, ordinance, Act of Parliament or other enactment having the force of law.[672] The phrase "enactment having the force of law" in this definition excludes precepts of the common law, as does the phrase "any other law" or phrases to a similar effect when used in statutes.[673] Statutes derive their binding force from their authors or "makers" authority.[674] This distinctive characteristic inevitably impacts how they are construed.[675] The Act has a generative or productive and not merely a classificatory function; it constitutes meaning and portrays the Act's purpose.

With the evolving technology and widespread use of cloud computing services, the legislature cannot keep up with the fourth industrial revolution[676] advances, at least for now. That could be the possible and logical reason why the POPI Act does not explicitly address a single form or mechanism of processing personal information and regulate each separately, such as cloud computing, spam, data mining, big data and cookies. It can only make sense that the legislator's intention by formulating section 3 was to provide a flexible statutory interpretation. The flexible interpretation approach would go beyond the ordinary and literal interpretation of the POPI Act's scope to address various forms of processing personal information.

In the 2013 matter of *Heroldt v Wills,*[677] Judge Willis commented that the technological progress has quickened to the extent that the social changes that result from there require high levels of skill from the courts and the lawyers who must respond

---

671 33 of 1957 section 2.

672 *R v Sutherland* 1961 (3) All SA 50 (A); *R v Sutherland* 1961 (2) SA 806 (A) para 814AB and *S v Kruger* 1968 (1) All SA 484 (T); *S v Kruger* 1968 (1) SA 507 (T) para 508F.

673 *Schuurman v Motor Insurers' Association of SA* 1960 (4) All SA 97 (T); 1960 (4) SA 316 (T) para 318B and *Torwood Properties v SA Reserve Bank* 1996 (1) SA 215 (W) para 226C "Common law" is often understood to be that body of law that is not statute law.

674 H H Hahlo and E Kahn *South African Legal System and its Background* (1969)143.

675 Du Plessis 2015 *Potchefstroom Electronic Law Journal* 1333 to 1334.

676 Fourth Industrial Revolution (4IR) is a fusion of advances in artificial intelligence (AI), robotics, the Internet of Things (IoT), genetic engineering, quantum computing, and more by D McGinnis "What is the Industrial Revolution?" (27 October 2020) *the 360 blog* https://www.salesforce.com/blog/what-is-the-fourth-industrial-revolution-4ir/ Accessed 26 February 2022)

677 2013 (2) SA 530 (GSJ) para 8.

appropriately. The Court went further to note that there is a "dearth of South African case law" [678] on Internet-based technologies. This comment supported the notion that laws need to be explored and interpreted accordingly in law courts to align with technology the growth.

To apply the POPI Act provisions in the cloud computing context, it is essential to understand and interpret specific terms used in the Act. Such statutory interpretation goes beyond their definitions in section 1 of the Act to establish its purpose. The interpretation of these terms may inform a broader theoretical position on an approach or trend in statutory interpretation in the cloud computing context.

4.5 Interpretation of key definitions

Section 1 of the POPI Act defines specific terms used differently from their ordinary or literal meanings to achieve their purpose when applied to cloud computing services. Given their meaning under section 1 of the POPI Act, these terms remain attached with different connotations. They, therefore, require different interpretation approaches to apply the legal opinions and judgments in the context of cloud computing services.

In the subsequent paragraphs, the following terms will be tested and explained in conjunction with the relevant sections of the POPI Act. These words are "processing", "record", "filing system", "personal information", "data subject", "responsible party", "electronic communication" and "automated means". This analysis will test whether POPI Act or certain sections thereof explicitly[679] regulate the use of cloud computing services. If not, what approach should the courts interpret the POPI Act to ensure that it regulates cloud computing services?

In terms of section 2 read with section 3(1)(a), it is paramount to highlight what aspects or categories of information or data fall under the phrase "personal information". Not all kinds of information could fall under the Act's scope, such as the personal

[678] *Heroldt v Wills* para 9.

[679] "Explicit" is defined as "stated clearly and in detail, leaving no room for confusion or doubt" or "very clear and exact not hiding anything"; South African School Dictionary 3rd Edition Oxford University Press South Africa at 215.

information processed in the course of purely household activities.[680] Information processed for journalistic, literary or artistic purposes.[681] Alternatively, any personal information that does not reveal or reveal the data subject's identity is also excluded in the POPI Act.

4.5.1 The meaning of "personal information"

Section 1 of the POPI Act defines personal information as information relating to an identifiable, living, natural person and an identifiable, existing juristic person.[682] In other words, personal information relating to a deceased natural person or a juristic person that no longer exists is not considered personal information in terms of the Act.[683] Personal information includes but is not limited to information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.[684]

The scope of personal information could further entail information relating to the education or the person's medical, financial, criminal or employment history.[685] Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignments to the person fall within the scope of personal information.[686]

The person's biometric information also relates to personal information in terms of the POPI Act mentioned under section 1. The person's personal opinions, views or preferences, correspondence sent by the person implicitly or explicitly of a private or confidential nature is part of personal information.[687] Further correspondence that would reveal the original correspondence's contents is also classified as personal

---

[680] Section 6 of the Protection of Personal Information Act.
[681] Section 7 of the Protection of Personal Information Act.
[682] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) (Ltd) v Smit* NO 2001 (1) SA 545 (CC) and Roos 2020 *Comparative and International Law Journal of Southern Africa* 9.
[683] Neethling *et al Neethling on Personality Rights* 375.
[684] Section 1 of the Protection of Personal Information Act.
[685] *Ibid*.
[686] *Ibid*.
[687] *Ibid*.

information under the Act.[688] The views or opinions of another individual about the person and the person's name, if it appears with other personal information relating to the person, is classified as personal information. If the disclosure of the name itself would reveal information about the person, all fall within the scope of "personal information" as defined in the POPI Act.[689]

The extension of personal information protection to juristic persons implies that they also have the right to privacy.[690] In the cases of *Financial Mail (Pty) Ltd v Sage Holdings Ltd*,[691] and *Universiteit van Pretoria v Tommie Meyer Films*,[692] the Court expanded the right to privacy to juristic persons. In Tommie Meyer's case, Rabie JA proceeded on the assumption that the appellant, a university, would in appropriate circumstances enjoy the right to privacy without deciding on the matter.[693] The same judgment was observed in *Dlomo NO v Natal Newspapers (Pty) Ltd*.[694] Personal information processing is only subject to the POPI Act if done by or for a responsible party.[695]

In the context of cloud computing and the right to privacy, a purposive approach to interpreting the definition of personal information is required. A purposive approach would provide a broad construction to apply its provisions to achieve the purpose of the legislation.[696] It would be absurd for the legislature to regulate personal information processing by following the common law interpretation approach under the *actio iniuriarum.* The *actio iniuriarum* requires that personal information processing's unlawfulness must be intentional rather than negligent.[697]

---

[688] *Ibid*.
[689] *Ibid*.
[690] *Ibid*.
[691] 133 to134.
[692] 456.
[693] *Ibid*.
[694] 1989 (1) SA 945 (A) para 952E to 953D.
[695] Section 3(1)(a) of the Protection of Personal Information Act.
[696] Mashinini 2020 *De Jure Law Journal* 151.
[697] *Bernstein v Bester* 1996 (2) SA 751 (CC), *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A), Neethling *et a Neethling's Law of Delict* 5, A Naude "*Data Protection in South Africa: The Impact of the Protection of Personal Information Act and Recent International Developments* (LLM Mini-dissertation, UP, 2014) 9, *Ngwenyama v Mayelane* 2012 (3) All SA 408 (SCA) 409 and Mashinini 2020 *De Jure Law Journal* 150.

The interpretative approaches should not narrow the Act's scope. Intentional and negligent wrongful processing of personal information regardless of the circumstances falls within the POPI Act's scope. The element of processing personal information which the POPI Act primarily regulates is present as illustrated in section 73, read with section 99(1) of the POPI Act. Section 99(1) states that a data subject or, at the data subject's request, the IR may institute a civil action for damages in a court having jurisdiction. The action is brought against a responsible party for breach of any provision of the POPI Act as referred to in section 73, whether or not there is intent or negligence on the responsible party.

The Act does not merely protect personal information per se; the protection is granted to the data subject to whom the personal information relates.[698] It is, therefore, essential to establish the meaning of a "data subject" as used in the Act in the cloud computing context. There must be a living natural or an existing juristic person for specific information to fall under the POPI Act regulations.

4.5.2 The meaning of a "data subject"

According to section 1 of the POPI Act, a data subject means the person to whom the personal information relates. It is important to note that the Act does not only protect the personal information of SA citizens or people domiciled in SA.[699] Before the Act applies, the connecting factor is either that the responsible party is domiciled in SA or that the responsible party uses automated or non-automated means in SA.[700] Therefore, a data subject may not be domiciled within the SA's territorial borders.[701]

In the cloud computing context and the value chain, interpretation of a data subject means the individual whose personal information is collected and stored in a cloud computing server.[702] Cloud computing service providers often access users' computers or install software on them, such as cookies, virtual machines, or browser

[698] Section 1 of the Protection of Personal Information Act.
[699] Neethling *et al Neethling on Personality Rights* 377.
[700] Section 3(1) of the Protection of Personal Information Act and Neethling *et al Neethling on Personality Rights* 377.
[701] Neethling *et al Neethling on Personality Rights* 377.
[702] S Zimmeck "The Information Privacy Law of Web Applications and Cloud Computing" (2012) 29 *Santa Clara Computer & High Technology Law Journal* 451 at 466.

extensions, to process personal information.[703] Sometimes, the data subject could simultaneously become both the data subject and the responsible party. This is primarily when they directly use cloud computing services such as iCloud, Google drive and social media platforms to process their personal information.

Data privacy law is the law that regulates all the stages of the processing of personal information. [704] POPI Act generally describes the administration of personal information as "processing"[705] collectively. Regardless of how information is being handled or administered, or at what stage of processing, the POPI Act refers to it as "processing".[706] The term "processing" is defined under section 1 of the POPI Act.[707]

4.5.3 Interpreting the meaning of "processing" in the context of cloud computing

According to section 1 of the POPI Act, the term "processing" means any operation or activity or any set of operations concerning personal information processing, whether or not by automatic means. Processing includes collecting, receiving, organising, collating, storage, updating or modification, retrieval, alteration and consultation. Disseminating personal information can also be done through transmission, distribution and making it available in any other form, such as entering personal information into a record.

The processing must be done by or for a responsible party using automated or non-automated means to fall within the scope of "processing".[708] Merging and linking personal information also falls within the ambit of processing personal information and the restriction and degradation of personal information. Even the final steps of handling information such as erasure or destruction of personal information amount to processing according to section 1 of the POPI Act.

---

[703] *Ibid*.
[704] Neethling *et al Neethling on Personality Rights* 365.
[705] The Preamble of the Protection of Personal Information Act.
[706] Section 1 of the Protection of Personal Information Act.
[707] Section 2(a) of the Protection of Personal Information Act.
[708] Section 3 of the Protection of Personal Information Act.

A literal interpretation of the word “processing” in conjunction with other words used in the above definition renders the use of cloud computing services under the POPI Act explicitly addressed. For instance, using cloud computing services, the most apparent forms of personal information processing include capturing biometric identifiers like fingerprints and voice recognition.[709]

On the one hand, the ordinary meaning of “collection”[710] refers to the action or process of gathering together or seeking to acquire items of a particular kind to use such collected material for various reasons.[711] On the other hand, the word “storage”[712] in the context of cloud computing services[713] means to retain for future electronic retrieval. In cloud computing services, personal information is stored on various servers for a more extended period and accessed at any time, which entails “storage”.[714] Such collection and storage would relate to personal information defined in the POPI Act.[715]

The phrase “dissemination by means of transmission”, as indicated in section 1 of the POPI Act under the definition of “processing”, will fall within the scope of cloud computing. Such processing of personal information involves transmission through “automated means” as defined in the POPI Act.[716] Though not explicitly stated in the POPI Act, the legislator intends to regulate any form of personal information processing, which involves using computer networks and transmission mechanisms.

In this context, an intentionalism and purposivism approach should be used to interpret the POPI Act. Furthermore, judicial activism[717] should be employed to determine the intention and the objective of the definition of the term “processing” in the context of

[709] Section 3(1) (a) of the Protection of Personal Information Act, Mashinini 2020 *De Jure Law Journal* 150 and Roos 2020 *Comparative and International Law Journal of Southern Africa* 8.
[710] South African Oxford School Dictionary 116.
[711] Mashinini 2020 *De Jure Law Journal* 150.
[712] South African Oxford School Dictionary 585.
[713] Mell “The NIST Definition of Cloud Computing” 2 and Hage “Cloud Computing - Storms on the Horizon” 2.
[714] Sullivan 2014 *Computer Law and Security Review* 138, Dixon 2012 *Judges Journal* 36 and Peihani 2017 *Singapore Journal of Legal Studies* 77.
[715] Mashinini 2020 *De Jure Law Journal* 150.
[716] Preston “Customers Fire a Few Shots at Cloud Computing” 52.
[717] du Plessis 2015 *Potchefstroom Electronic Law Journal* 1335.

cloud computing. Such determination can be achieved through the expansion of the judicial statutory interpretation scope.[718] *Farrar's Estate v Commissioner's case for Inland Revenue* supports the intentionalism statutory interpretation approach.[719] The Court laid down the principle that in cases involving the interpretation of the statute, *dicta* to the effect that the real intention of the legislature must be determined and given effect to, are almost certain to occur.[720]

However, du Plessis[721] states that the judicial theory is a "free" theory of statutory interpretation. Its moderate form recognises, justifies, and strongly advocates judicial activism in its more radical form. It is premised on the belief that judges have a creative role in interpreting and applying statute law.

The "moderates" contend that ascertaining the legislature's intention entails filling in gaps in an enactment.[722] Thereby making sense of the provision rather than opening it up to destructive analysis. They do not favour adopting a "wait and see" attitude concerning legislative reform.[723] With the common law's help, the judiciary must intervene to remedy defects in statute law.[724] The judicial intervention is adopted since legislative processes are not sufficiently expeditious and streamlined to cope with deficiencies that show up in day-to-day practice.[725]

[718] *Shaw v Director of Public Prosecutions* 1961 (2) All ER 446 (HL) 452 to 453.
[719] 1926 TPD 501 508.
[720] *Ibid*, *Ensor v Rensco Motors (Pty) Ltd* 50 1981(1) SA 815(A) and *Engels v Allied Chemical Manufacturers (Pty) Ltd* 1993(4) SA 45(NM) 160.
[721] Du Plessis 2015 *Potchefstroom Electronic Law Journal* 1335.
[722] Lord Denning in *Magor & St Mellons Rural District Council v Newport Corporation* 1950 2 All ER 1226 (CA) 1236, Singh *The Impact of the Constitution on Transforming the Process of Statutory Interpretation in South Africa* 62 and Du Plessis *Re-Interpretation of Statutes* 97 (Du Plessis uses an interesting term to describe the judicial or the free theory. He refers to the judicial theory as 'judicial activism.').
[723] *Shaw v Director of Public Prosecutions* 1961 2 All ER 446 (HL) 452 to 453.
[724] Singh *The Impact of the Constitution on Transforming the Process of Statutory Interpretation in South Africa* 62 and Du Plessis *Re-Interpretation of Statutes* at 97.
[725] Devenish *Interpretation of Statutes* 48 to 49.

The terms "merging" [726] and "linking" [727] provide a complicated scenario when interpreting the Act in this context. When interpreting these terms, the courts must consider the facts on a case-by-case basis. The literal meanings of these terms as ordinarily defined and applied to cloud computing may produce an interpretive result so absurd and repugnant to common sense that the legislature could hardly be believed to have intended it.[728] The Court will then have to expand the interpretation of words beyond their ordinary meaning to attach the Act's intention, purpose, and application.

In cloud computing services, every information processed gets stored in one server with the rest of the data subjects' personal information. That could entail "merging" or "linking" personal information from different data subjects. To determine which responsible party is liable for the breach could pose a challenge considering various defences against an action for damages raised by each responsible party involved. These defences are set out under section 99(2) of the Act and the technical complexes associated with cloud computing and cyberspace in general.[729]

The Preamble of the POPI Act states that it aims to promote the protection of personal information processed by public[730] and private bodies[731]. These bodies are what the POPI Act refers to as a "responsible party". These are the parties who process

[726] The Term "merging" means "to join together with something else" South African Oxford School Dictionary 381.
[727] The term "linking" means "something that joins things or people together" or "a place where one electronic document on the internet is connected to another one" South African Oxford School Dictionary 354.
[728] *Grey v Pearson* 1843-60 All ER Rep 21 (HL) para 36.
[729] Section 99(2) of the Protection of Personal Information Act, Rosenzweig 2013 *Santa Barbara Praeger Security International* 78 and Lipson "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues" 14, Muir 2009 *ACM Computer Survey* 14 to 15 and Brown 2015 *International Journal of Cyber Criminology* 80.
[730] Section 1 of the Protection of Personal Information Act defines "public body" as—
(*a*) any department of State or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
(*b*) any other functionary or institution when—
(i) exercising a power or performing a duty in terms of the Constitution or a provincial Constitution; or
(ii) exercising a public power or performing a public function in terms of any legislation;
[731] Section 1 of the Protection of Personal Information Act defines a "private body" as—
(*a*) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
(*b*) a partnership which carries or has carried on any trade, business or profession; or
(c) any former or existing juristic person but excludes a public body.

personal information related to the data subject. The Act's purpose is to regulate how these bodies process personal information and provide remedial mechanisms for the data subjects whose personal information has been processed unlawfully.

4.5.4 Interpreting the meaning of a "responsible party"

The responsible party referred to in the POPI Act is a juristic person in the form of a private or public body that determines the purpose of processing personal information.[732] The legislator preferred the term; it was borrowed from the Dutch Personal Data Protection Act 2000.[733] The statutory provisions expressly restrict its jurisdiction to organisations and do not extend to private persons. This definition immediately excludes personal information processing by private individuals using cloud computing services from the POPI Act scope. It is somewhat understandable because the penalties for contravening the POPI Act may be too harsh for a private individual to bear for unlawfully processing personal information using cloud computing services.[734]

Nevertheless, juristic persons who use cloud computing services for processing personal information still fall within the scope of the meaning of a "responsible party". The Act's provisions will apply if they are processing personal information as defined in the POPI Act, using automated means (cloud computing). Private individuals who process personal information in that capacity are further protected by section 6 of the Act. Such processing must purely fall under personal or household activity described by section 6 of the POPI Act.

Notwithstanding that, it can be argued, however, that the phrase "… any other person which alone or in conjunction with others…" as used under the definition of "responsible party" could include private persons as well. Based on this interpretation, private persons are not entirely excluded from the provisions of the POPI Act. It is yet

[732] Section 1 of the Protection of Personal Information Act and Mashinini 2020 *De Jure Law Journal* 153.
[733] Neethling *et al Neethling on Personality Rights* 368.
[734] Section 107, read with section 109 of the Protection of Personal Information Act, provides penalties in the form of imprisonment or a fine not exceeding R10 million and Mashinini 2020 *De Jure Law Journal* 154.

to be seen how the IR will impose penalties on private individuals. It is also yet to be seen what criteria will be employed to differentiate between private individuals from public or private bodies as far as penalties are concerned.

4.5.4.1 The conditions for lawful processing of personal information by responsible parties in terms of the POPI Act

This study section will not provide an extensive analysis of the conditions for the lawful processing of personal information. The time and space allocated for this research are minimal to cover all the provisions of the POPI Act. However, to archive the purpose and scope of this research, the eight conditions for the lawful processing of personal information will be discussed briefly. The discussion will also be necessary as the processing of personal information by the responsible parties can only be done lawfully if they comply with those conditions.

The responsible party must ensure that the conditions set out in Chapter 3 and all the measures that give effect to such conditions are complied with at the time of the determination of the purpose and means of the processing and during the processing of personal information itself.[735] The POPI Act assigns accountability explicitly for lawful data processing to the responsible party.[736] The provisions hold the responsible party accountable for non-compliance with the POPI Act.[737]

The responsible party will be accountable for any interference with protecting the personal information of a data subject and liable for any breach of the principles.[738] This principle is self-evident and in line with the common law position that the person processing personal information can receive a prohibitory or mandatory interdict or be

[735] Section 4(1) of and 8 of the Protection of Personal Information Act.
[736] Section 8 of the Protection of Personal Information Act.
[737] Section 99(1) of the Protection of Personal Information Act, *Tobani v Minister of Correctional Services* 2002 (2) All SA 318 (SEC) 326 to 327, *Minister of Correctional Services v Tobani* 2003 (5) SA 126 (E) 133 to 137 and *Sex Worker Education and Advocacy Task Force (SWEAT) v Minister of Safety and Security* 2009 (6) SA 513 (WCC) 523.
[738] Chapter 3; Condition 2; section 9 of the Protection of Personal Information Act reads that; Lawfulness of processing. —Personal information must be processed—
(*a*) lawfully, and
(*b*) in a reasonable manner that does not infringe the data subject's privacy and Sections 99 and 107 of the Protection of Personal Information Act.

liable and accountable for the unlawful infringement of privacy identity.[739] Whereas intent and wrongfulness are a requirement for common-law liability, liability is strict liability according to the POPI Act.[740]

Personal information must be processed lawfully and reasonably that does not infringe the data subject's privacy.[741] The responsible party must further ensure that personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.[742] Section 13 entails that personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. When the purpose has been established, further processing of personal information must be in accordance or compatible with the purpose for which it was collected.[743]

Section 16(1) provides that a responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary. While section 16(2) entails that in taking the steps referred to in section 16(1), the responsible party must have regard to the purpose for which personal information is collected or further processed. Such a responsible party must maintain the documentation of all processing operations under its responsibility.[744]

Section 19 provides that a responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information.[745] The security measure must also prevent unlawful access to or processing personal information by third parties.[746] A cloud computing service provider's protection measures are

[739] Neethling *et al Neethling's Law of Personality* 278.
[740] Millard 2016 *Potchefstroom Electronic Law Journal* 3.
[741] Section 9 of the Protection of Personal Information Act.
[742] Section 10 of the Protection of Personal Information Act.
[743] Section 15 of the Protection of Personal Information Act.
[744] Section 17 of the Protection of Personal Information Act.
[745] Section 19(1)(a) of the Protection of Personal Information Act.
[746] Section 19(1)(b) of the Protection of Personal Information Act.

inadequate if the cloud computing client does not control the organisational and technical measures that the cloud service provider has deployed.[747]

In all of this, the responsible party must ensure that a data subject, having provided adequate proof of identity, has the right to request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject.[748] The data subject also has a right to request from a responsible party the record or a description of the personal information about the data subject held by the responsible party.[749] This includes personal information about the identity of all third parties, or categories of third parties, who have or have had access to the information[750]

If these conditions are not adhered to by the responsible party, data subjects have the right to lodge a claim or raise a dispute to achieve a remedy in terms of section 99.[751] The IR may also intervene by requesting or enforcing the blocking, erasure or destruction of data or even shutting off the operator's system.[752] It is essential that the responsible party effectively control the cloud computing service provider and use the IT systems to influence or stop the data processing.[753]

In terms of the law of delict, private data processors can be directly and vicariously liable, while the state can only be vicariously liable.[754] Since the Act does not distinguish between the state and private responsible parties, it is debatable whether the state can be directly liable for breach of the protection principles when using cloud

[747] *Ibid*.
[748] Section 23(1)(a) of the Protection of Personal Information Act.
[749] Section 23(1)(b) of the Protection of Personal Information Act.
[750] *Ibid*.
[751] Section 99 of the Protection of Personal Information Act; Civil remedies: — (1) A data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act as referred to in section 73, whether or not there is intent or negligence on the part of the responsible party.
[752] Section 40 of the Protection of Personal Information Act.
[753] IT Governance Network "Impact of the POPI Act on Cloud Computing" 2013 http://www.itgovernance.co.za (Accessed 10 March 2021).
[754] Section 1 of the State Liability Act 20 of 1957 provides that the state is liable for "any wrong committed by any servant of the State acting in his capacity and within the scope of his authority as such a servant". Seen thus, the state can only be vicariously liable for the delicts of its employees, Midgley *et al Delict* 257 to 258, Neethling *et al Neethling's Law of Delict* 368, *Masuku v Mdlalose* 1998 (1) SA 1 (A) para 14 to16 and *Mhlongo v Minister of Police* 1978 (2) SA 551 (A) 567.

computing services. Finally, a distinct fundamental difference between the law of delict and the POPI Act is that the IR ensures that responsible parties adhere to the data protection principles.[755] The data subjects themselves must enforce their privacy and identity protection against the data industry's activities by being actively involved in the common law.[756]

For the Act's provisions to apply, the responsible party could be domiciled in the Republic or not domiciled in the Republic but makes use of automated means.[757] Such automated means include using cloud computing services in this context in the Republic unless used only to forward personal information through the Republic.[758] It is vital to analyse the term "record" in the cloud computing context to determine how it relates to the processing of personal information using cloud computing services under the provisions of the POPI Act.

4.5.5 The interpretation of the term "record" in the context of cloud computing

In terms of section 1 of the POPI Act, as defined, the term "record" means any recorded information regardless of form or medium used to record such information. The term record includes writing on any material, label, marking or other writing that identifies or describes anything it forms part. Any information to which it is attached by any means of a book, map, plan, graph or drawing, photograph, film, negative, tape fall within the scope of a "record".

Other devices in which one or more visual images are embodied to be capable, with or without the aid of some additional equipment, of being reproduced is also classified as a "record".[759] A record is further described as any information which could be in the

[755] Section 40(1)(a)(i) of the Protection of Personal Information Act on Powers, duties and functions of the Information Regulator provides that in terms of the Act, the Information Regulator has to provide education by promoting an understanding and acceptance of the conditions for the lawful processing of personal information and the objects of those conditions.
[756] Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 644 to 649, Neethling *et al Neethling's Law of Personality* 278 to 280 and Neethling 2012 *THRHR* 245.
[757] Section 3(b) and section 72 of the Protection of Personal Information Act.
[758] Section 3(1)(a) and (b)(i)(ii) of the Protection of Personal Information Act.
[759] Section 1 of the Protection of Personal Information Act.

possession or under the control of a responsible party. This is regardless of whether or not a responsible party created it or when it came into existence.[760]

The POPI Act provides that information produced or recorded using computer equipment, whether hardware or software, refers to a record, regardless of form or medium.[761] Cloud computing uses computer equipment, software, and specific hardware to process personal information. Executing such a processing mechanism falls within the scope of a "record" in the POPI Act. Therefore, the responsible party must ensure that the processing of personal information stored in a record follows the POPI Act's provisions.

4.5.6 Meaning of "automated means" in terms of cloud computing services configuration

It is essential to mention that the phrase "automated means" as frequently used in the POPI Act is not defined under section 1. In terms of section 3(4), for the POPI Act, "automated means" is described as any equipment capable of operating automatically in response to instructions given for processing personal information.

The POPI Act applies to information processing using "automated" and "non-automated" means. It seems that the legislature intended to include any possible automated means that could be used by a responsible party to process personal information (including cloud computing services). Automated equipment must respond to instructions sent to it, but without physical human intervention except sending a command.[762] Therefore, the processing of personal information using cloud computing services amounts to processing using automated means.

If such processing falls under non-automated means as provided for under Section 3(1)(a), the use of cloud computing will still be within the scope of the POPI Act,[763] provided that when the recorded personal information is processed by non-automated

[760] *Ibid.*
[761] *Ibid* and Mashinini 2020 *De Jure Law Journal* 153.
[762] Section 1 of the Protection of Personal Information Act and Mashinini 2020 *De Jure Law Journal* 153.
[763] Mashinini 2020 *De Jure Law Journal* 154.

means, it forms part of a filing system or is intended to form part. Using the statutory interpretation approach, the phrase “filing system” will be interpreted in relation to cloud computing services.

4.5.7 Interpreting the meaning of a “filing system” in the context of cloud computing

In terms of section 1 of the POPI Act, “filing system” means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.[764] Personal information can be stored on a database, server or network, as the data can be centralised, decentralised or dispersed on a functional and geographical basis.[765]

Cloud computing services have a filing system used to collect and store all the information processed by the operator[766] for or on behalf of the responsible party. The cloud computing operator feeds the information to a computerised gadget and sends a command to the device. The device then provides a live feed to a network that will transmit the information to the cloud computing service provider’s server.[767] Such information is then stored on a server and released in response to demand.[768]

The term “centralised” addresses the information storage mechanisms of personal information in the cloud computing servers. Once the data has been processed in the cloud computing servers, the data gets mixed “as if in the cloud”. The process pools different pieces of information and “file” them in one server. One server could store information from multiple clients, therefore “centralising” personal information. The burden then lies on cloud computing service providers to minimise the risks of data breaches.[769]

The cross-border flow of personal information characteristic of cloud computing covers the section of the definition “…whether personal information is centralised,

---

[764] Section 1 of the Protection of Personal Information Act.
[765] *Ibid*.
[766] *Ibid* defines “operator” as a person who processes personal information for a responsible party in terms of a contract or mandate without coming under that party's direct authority.
[767] Clarke 2014 *Computer and Security Law Review* 287 and Mashinini 2020 *De Jure Law Journal* 154.
[768] Sullivan 2014 *Computer Law and Security Review* 137 at 138, Dixon 2012 *Judges Journal* 36 and Peihani 2017 *Singapore Journal of Legal Studies* 77.
[769] *Ibid* and Sections 19 to 22 of the Protection of Personal Information Act.

decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria".

To execute the processing of personal information, Cloud computing services should make use of electronic gadgets. The electronic device requires a communications network to transmit information to the servers. It is for this reason to provide a statutory interpretation of the term "electronic communication" below in the cloud computing context.

4.5.8 The meaning of "electronic communication" and its application to cloud computing

In terms of section 1 of the POPI Act, "electronic communication" means: -

> "any text, voice, sound or image message sent over an electronic communications network which is stored in the network or the recipient's terminal equipment until the recipient collects it."

This definition covers the scope of the systematic design and use of cloud computing services. For instance, exchanging or processing personal information on social media such as photos, "images", voice notes, "voice", music or recordings, "sound", messages or emails "text' that utilises cloud computing services to administer its day-to-day operations. These services must further use computerised electronic gadgets to process and transmit such information, which falls within the scope of the phrase "electronic communication". Theoretically, cloud computing could be summarised under electronic services if the activity sends signals over electronic communications networks.[770]

The use of a "network" is covered under the definition of "electronic communication" and cloud computing. This entails that the Act explicitly protects this part of cloud computing. With a purposive approach and judicial activism, "recipient's terminal equipment" means a "server" in the context of cloud computing.

[770] Sluljs *et al* "Cloud Computing in the EU Policy Sphere Interoperability, Vertical Integration and the Internal Market".

The last part of the definition states that "… until the recipient collects it". This part of the definition covers the definition of cloud computing, which states that an individual can easily access the information stored in the cloud computing service provider's servers at any time on demand.

Since cloud computing service providers offer IT related services enabling the storing and processing of data, it can be argued that they are dependent on the Internet service providers to facilitate the sending and receiving signals on the networks. Cloud computing service providers are not establishing the communications infrastructure. They are also not associated with the respective services, meaning that regulations on electronic communications do not hit the core of cloud computing services.[771] Nevertheless, this technical assessment does not mean that a cloud computing service provider exercises editorial control over any content transmitted.[772]

The courts should promote and protect the right to privacy using a purposive approach, as any conflicting interpretation can misrepresent the POPI Act's purpose. Nevertheless, the legislature has included a list of activities excluded from the meaning of personal information to curb the far-reaching effects of the purposive approach.[773] The POPI Act provides for exclusion, exemption and exception from the purposes of the POPI Act'[774] Certain processing activities are entirely excluded from the POPI Act's provisions with exclusions.[775] Exclusions, exemptions and exceptions are allowed where processing only poses a small risk to the data subject's privacy or where overriding interests of other persons have to be taken into account.[776]

4.6 Exclusions and exceptions of certain personal information

This section deals with excluding purely household activities or personal activities from the scope of personal information.[777] In terms of section 6,[778] the POPI Act does not

[771] Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 44.
[772] *Ibid*.
[773] Mashinini 2020 *De Jure Law Journal* 151.
[774] Neethling *et al Neethling on Personality Rights* 378.
[775] *Ibid.*
[776] *Ibid* and Roos 2006 *CILSA* 127 to 129.
[777] Neethling 2012 *THRHR* 246.
[778] The date of commencement of section 6 was 1 July 2020.

apply to the processing of personal information in the course of a purely personal or household activity that has been de-identified[779] to the extent that it cannot be re-identified[780] again.[781] The exclusion of such personal information is applicable if the processing is done by or on behalf of a public body.[782] The Act does not regulate this activity since the risk posed to third parties' privacy is minimal.[783]

Under section 6(c), to exclude such personal information processed using cloud computing services in terms of the POPI Act, the information must involve national security.[784] Such activities assist in identifying the financing of terrorist and related activities, defence or public safety.[785]

The purpose of such exclusion is to provide further; prevention and detection, including assistance in identifying the proceeds of unlawful activities. The illegal activities include combating money laundering activities, investigation, or proof of offences.[786] To the extent that adequate safeguards have been established in legislation to protect such personal information, the prosecution of offenders or the execution of sentences or security measures is also excluded.[787] The Cabinet and its committees or the Executive Council of a province in that capacity are vested with such powers to enforce section 6(c). Section 6(1)(d) states that the exclusion must relate to a court's judicial functions, which is also discussed and referred to in section 166 of the Constitution.[788]

---

[779] Section 1 of the Protection of Personal Information Act defines "de-identify", concerning the processing of personal information of a data subject, means to delete any information that—
(*a*) identifies the data subject;
(*b*) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
(*c*) A reasonably foreseeable method can be linked to other information that identifies the data subject, and "re-identified" has a corresponding meaning.

[780] Section 1 of the Protection of Personal Information Act defines "re-identify", concerning the processing of personal information of a data subject, means to resurrect any de-identified information, that—
(*a*) identifies the data subject;
(*b*) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
(*c*) A reasonably foreseeable method can be linked to other information that identifies the data subject and "de-identified" has a corresponding meaning.

[781] Section 6(1)(a) and (b) of the Protection of Personal Information Act.

[782] Section 6(1)(c) of the Protection of Personal Information Act.

[783] Neethling *et al Neethling on Personality Rights* 378.

[784] Section 6(1)(c)(i) of the Protection of Personal Information Act.

[785] *Ibid*.

[786] Section 6(1)(c)(ii) of the Protection of Personal Information Act.

[787] *Ibid.*

[788] Section 6(1)(e) of the Protection of Personal Information Act.

The phrase “household or personal activities” is not defined under section 1 or anywhere in the POPI Act. The exclusion of the household or personal activities under the POPI Act creates a gap in its scope. For instance, if an ordinary natural person posts photography of another data subject on social media that use cloud computing services within the same household without the latter’s consent, section 6 will be applicable as this could form or fall under the “household or personal activities”.

Another example could be when an adult posts pictures of their family on Instagram, however, they gain popularity and earn substantial advertising revenue from their blog in the process. There is arguably some connection to professional or commercial activity, but the household exemption may still apply since section 6 of the POPI Act does not refer to commercial activity. Under certain circumstances, the processing of activities may cross the line of purely household purposes, in which case the exclusion is not applicable.[789]

Violations of the right to privacy and serious consequences may arise if the photograph posted on social media concerning another data subject under the provisions of “personal household activities” using cloud computing services is excluded from the POPI Act provisions. The right to privacy would erode if a purposive approach is not applied, and any conflicting interpretation would thwart the Constitution’s spirit, purport, and values.[790]

As people’s day-to-day household activities do not amount to processing personal information within the meaning of the POPI Act, the right to privacy may be violated.[791] Personal activities may range from everything a data subject does with their life, save for actions undertaken in the workplace or at a public event.[792] Considering what may be viewed subjectively as “personal activities”, it appears that the meaning of “personal

[789] Neethling *et al Neethling on Personality Rights* 378 and Roos 2006 *CILSA* 127 to 129.
[790] Mashinini 2020 *De Jure Law Journal* 151.
[791] Section 6 of the Protection of Personal Information Act.
[792] Mashinini 2020 *De Jure Law Journal* 151.

activities" is broad or unfairly limited under the scope and the purpose of the POPI Act.[793]

The meaning of the phrase "household or personal activities" must be viewed objectively and reasonably in line with the community's legal convictions.[794] What is "personal" may differ from person to person, as everyone has the right to "determine what they would like to keep private".[795] Drawing a line between what is and what is not purely personal household activity may be difficult in some instances. This will depend on the court's approach to interpret the statute or the specific "personal activity" in question. The exclusion of purely household activities in section 6 of the POPI Act remains to be tested in court or addressed by the IR when determining personal information margins.[796]

The POPI Act provides for the establishment of an IR to exercise certain powers and perform specific duties and functions in terms of the POPI Act.[797] The meaning and the scope of the IR will be discussed in the paragraphs below.

4.7 The establishment of the Information Regulator

According to section 39 of the Act,[798] the legislature included the provisions of establishing the Information Regulator.[799] The IR has jurisdiction throughout the Republic as far as the processing of personal information is concerned with the Act.[800] It is independent and subject only to the Constitution and the law.[801] The IR must be impartial, perform its functions and exercise its powers without fear, favour or prejudice.[802] The Act further provides the IR with authority to exercise its powers and

[793] *Ibid*.
[794] Neethling *et al Neethling's Law of Delict* 55 (Determining the community's legal convictions requires a constitutionally transformative approach because the Constitution applies to all law). Therefore, the meaning of "personal activities" must be informed by the norms and values underpinning the Republic of South Africa Constitution, 1996 and Mashinini 2020 *De Jure Law Journal* 152.
[795] Mashinini 2020 *De Jure Law Journal* 152.
[796] *Ibid*.
[797] The Preamble of the Protection of Personal Information Act.
[798] The date of commencement of section 39 was 11 April 2014.
[799] Section 1 of the Protection of Personal Information Act defines the "Regulator" as the Information Regulator established in section 39 of the Protection of Personal Information Act.
[800] Section 39(a) of the Protection of Personal Information Act.
[801] Section 39(b) of the Protection of Personal Information Act.
[802] *Ibid*.

perform its functions according to the POPI Act and is only accountable to the National Assembly.[803]The IR is responsible for the oversight for implementing the POPI Act, and it is assisted by the information officers that have to be appointed by every responsible party.[804]

4.7.1 The powers, duties and functions of the Information Regulator

Section 40 of the POPI Act deals with the appointment of the IR by the government. The IR is responsible for South African businesses and the public regarding their responsibilities and rights on personal information protection.[805] The IR is also responsible for the monitoring and enforcement of adherence to the POPI Act.[806] It handles complaints regarding privacy violations, conducts research, and issues codes of conduct, where required.[807] Facilitating cross-border cooperation between different countries in terms of various privacy laws also falls within the IR scope.[808]

The IR also consults with the interested parties by, among other things receiving and inviting representations from the members of the public and any matters affecting the personal information of the data subjects.[809] The IR corporates with national and international bodies concerned with protecting personal information.[810] The IR also act as a mediator between opposing parties on any matter that concerns the processing of personal information.[811]

The IR may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this POPI Act as referred to in section 73. The civil action can be brought against the responsible party whether or not there is intent or negligence.

[803] Section 39(c) and (d) of the Protection of Personal Information Act.
[804] Section 55 of the Protection of Personal Information Act.
[805] Section 40(1)(a) of the Protection of Personal Information Act.
[806] Section 40(1)(b) of the Protection of Personal Information Act.
[807] *Ibid*.
[808] Section 40(1)(b), (d), (e), (f) and (g) of the Protection of Personal Information Act.
[809] Section 40(1)(c)(i) of the Protection of Personal Information Act.
[810] Section 40(1)(c)(ii) of the Protection of Personal Information Act.
[811] Section 40(1)(c)(iii) of the Protection of Personal Information Act.

According to sections 107[812] and 109,[813] the POPI Act determines that the IR have powers to impose a fine of up to R 10 million or imprisonment that does not exceed 10 years or a fine and incarceration combined. The possible monetary fines and imprisonment with the additional prospect of reputational damage pose a clear threat to South African businesses. These sanctions apply to public and private institutions if they breach the POPI Act's provisions.

Where data subjects do not consent to use their personal information or where customers of a business have requested its removal from the database in question, the data subject could seek a remedy through the IR. Responsible parties who use cloud computing services to process such personal information will be in contravention of the Act and subject to the jurisdiction of the IR.

Consequently, when transacting on the Internet, personal information is now theoretically safe with South African companies. Responsible parties using cloud computing services are bound to national legislation and the POPI Act in particular. It will be interesting to watch how the IR's compliance, enforcement, and penalties unfold and precisely understand what process must be followed when complaining about international data breaches.[814]

4.7.2 Jurisdiction of the Information Regulator

[812] Section 107 of the Protection of Personal Information Act provide provisions for Penalties in the following manner: Any person convicted of an offence in terms of this Act is liable, in the case of an infringement of—
(*a*) section 100, 103 (1), 104 (2), 105 (1), 106 (1), (3) or (4) to a fine or imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment; or
(*b*) section 59, 101, 102, 103 (2) or 104 (1), to a fine or imprisonment for a period not exceeding 12 months or both a fine and such imprisonment.
[813] Section 109 of the Protection of Personal Information Act provide provisions for Administrative fines as follows (1) If a responsible party is alleged to have committed an offence in terms of this Act, the Regulator may cause to be delivered by hand to that person (hereinafter referred to as the infringer) an infringement notice which must contain the particulars contemplated in subsection (2).
[814] Swales 2016 *South African Mercantile Law Journal* 76.

Section 40 requires the Information Regulator to monitor and enforce compliance in public and private sectors.[815] Then section 40(1)(b)(ii) legislates explicitly that the IR must:-

> "research into, and monitor developments in information processing and computer technology to ensure that any adverse effects of such developments on the protection of the personal information of data subjects are minimised and reporting to the Minister the results of such research and monitoring".

The developments of cloud computing services are addressed under this section of the POPI Act. The IR should play a critical, grassroots role in understanding the nature and scope of the complaints related to data breaches, specifically in cloud computing services. The IR must observe a balance between the right to privacy with economic activities in the marketplace. In section 57(1), the responsible party must obtain prior authorisation from the IR before processing if the responsible party plans to.

Though not explicitly covered under this section, an intentionalism statutory interpretation approach should be employed to interpret the provisions of section 40. The legislator intended to regulate any computerised data processing mechanism, which includes cloud computing services. In terms of section 40(1)(b)(ii), the phrase "information processing and computer technology" will cover cloud computing.

In summary, in terms of chapter 5 of the Act, sections 39 to 56, the IR is empowered to search and seize, impose administrative fines and sue on behalf of the data subjects. The IR also determines whether the law is being complied with, receive and act upon any complaints, and may issue notices of non-compliance.[816]

4.7.3 Procedure for dealing with complaints

[815] Section 40 (1)(b)(i) of the Protection of Personal Information Act states that the Information Regulator has to monitor and enforce compliance by - public and private bodies with the provisions of this Act (POPI Act).
[816] Swales 2016 *South African Mercantile Law Journal* 77.

The IR deals with issuing codes of conduct among its other duties and functions.[817] Section 63 then provides that a code of conduct may prescribe procedures for making and dealing with complaints alleging a breach of the code, but no such provision may limit or restrict any provision of Chapter 10.[818] If the code sets out procedures for making and dealing with complaints, the IR must be satisfied that the procedures meet the prescribed standards.[819] The IR must also be satisfied that the guidelines issued by the IR in terms of section 65,[820] relate to the making of and dealing with complaints. Section 63(2)(b) states that IR must be satisfied that the code provides for the appointment of an independent adjudicator to whom complaints may be made.

The code provides that, in exercising their powers and performing their functions, under the code, an adjudicator for the code must have due regard to the matters listed in section 44.[821] The codes of conduct require the adjudicator to prepare and submit a report, in a form satisfactory to the IR within five months of the end of a financial year of the IR on the operation of the code during that financial year.[822] The code requires the report prepared for each year to specify the number and nature of complaints made to an adjudicator under the code during the relevant financial year.[823]

A responsible party or data subject who is aggrieved by a determination, including any declaration, order or direction included in the determination made by an adjudicator, can still challenge such an outcome. After investigating a complaint relating to the protection of personal information under an approved code of conduct, the affected party may submit a complaint in terms of section 74 (2) with the IR against the determination upon payment of a prescribed fee.[824] The adjudicator's determination continues to have effect unless and until the IR decides under Chapter 10 relating to the complaint or unless the IR determines otherwise.[825]

---

[817] Section 40(1)(f) and Chapter 7 of the Protection of Personal Information Act.
[818] Chapter 10 deals with the enforcement mechanisms of the POPI Act by the IR.
[819] Section 63(2)(a) of the Protection of Personal Information Act.
[820] Section 65 deals with the guidelines about the codes of conduct.
[821] Section 63(2)(c) of the Protection of Personal Information Act; section 44 of the Act deals with the IR regarding certain matters on the lawful processing of personal information.
[822] Section 63(2)(d) of the Protection of Personal Information Act.
[823] Section 63(2)(e) of the Protection of Personal Information Act.
[824] Section 63(3) of the Protection of Personal Information Act.
[825] Section 63(4) of the Protection of Personal Information Act.

As much as the IR has the powers to promote personal information protection, section 77[826] gives the IR discretion to decide to take no action on specific complaints. An analysis of section 77 in the cloud computing context is discussed below.

4.8 The discretion of the Information Regulator on a complaint

In terms of section 77(1), the IR may decide to take no action on a complaint brought before it by a data subject or on behalf of a data subject for the unlawful processing of personal information using cloud computing services.[827] This provision applies to the IR after investigating a complaint received in terms of section 73.[828] The IR may then decide to take no action or, as the case may be, require no further action regarding the complaint. If in the IR's opinion, the length of time that had elapsed between the date when the subject matter of the complaint arose and the date when the complaint was made is excessive or too prolonged, it may take no action.[829]

Section 77 (1)(a) raises a challenge in the context of cloud computing and poses unfairness to data subjects. Cloud computing can store vast amounts of personal information for a highly extended period. For instance, if the information has been stored in the cloud computing service provider servers for 10 years, during that period, the cloud computing service provider gets breached, and the responsible party fails to notify the data subject about the breach as prescribed by the Act. Then the data subject only becomes aware of such a breach because some illegal activities have been perpetrated by the hackers later in the years using the data subject's personal information obtained unlawfully. This then entails that the responsible party could evade liability. The IR may decide not to take action on such a complaint in terms of section 77(1)(a), citing the elapsed time. The data subject will be left with no redress in this context, forcing them to rely on other available remedies except the POPI Act and the use of the IR's remedies.

[826] The commencement date of section 77 was 1 July 2020 as per the Protection of Personal Information Act Proclamation, GN R21, *Government Gazette* 43461, 22 June 2020.
[827] Also, section 76(1)(c) of the Protection of Personal Information Act provides a similar provision.
[828] Section 77(1) of the Protection of Personal Information Act.
[829] Section 77(1)(a) of the Protection of Personal Information Act.

Although Section 39(1)(a) provides that the IR has Jurisdiction throughout the Republic, it seems like its jurisdiction does not extend beyond the territorial borders of SA. Since the IR has to exercise its powers in terms of the POPI Act, its jurisdiction could extend extraterritorial in circumstances where personal information is processed by or to a third party in a foreign country.[830]

Many data protection legislation across the world make provision for cross-border transfers of personal information, such as the GDPR.[831] To meet data protection standards set by the EU's GDPR, SA's POPI Act has to regulate the trans-border flows of personal information to countries without adequate data privacy protection laws.[832] The common standard for data transfer is an "adequate" level of data protection in the receiving country, however, there are exceptions, such as contracts and consent of the data subject.[833] The POPI Act makes provisions for cross-border personal information transfer under section 72. A detailed discussion of section 72 in the context of cloud computing is provided below.

4.9 Transfer of personal information outside the Republic

Section 72 of the POPI Act outlines the provisions for transferring personal information outside the Republic using cloud computing services.[834] Section 72(1) provides that a responsible party in the Republic may not transfer personal information using cloud computing services about data subject to the third party in a foreign country.[835]

The transfer of information cannot be done unless the third party who is the recipient of the information is subject to a law, binding corporate rules or the binding agreement that provides an adequate protection level.[836] Such rules and agreements must effectively uphold principles for reasonable processing of personal information as

[830] Section 72(1) of the Protection of Personal Information Act.
[831] Baloyi "Are Organizations in South Africa Ready to Comply with Personal Data Protection or Privacy Legislation and Regulations?" 6.
[832] Neethling *et al Neethling on Personality Rights* 406.
[833] *Ibid*.
[834] The date of commencement of section 72 was 1 July 2020.
[835] Section 72(1) of the Protection of Personal Information Act.
[836] Section 72(1)(a) of the Protection of Personal Information Act.

outlined in the Act.[837] The processing principles must be substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person in terms of the POPI Act.[838]

To obtain validation as binding corporate rules or agreements that provide an adequate data protection level, corporate regulations and agreements should include provisions substantially similar to section 72 of the POPI Act.[839] The provision of section 72(1)(a)(ii) relate to the further transfer of personal information from the recipient to third parties who are in a foreign country.[840] The condition is that the processed personal information will be subject to adequate data privacy protection rules in a foreign country.[841]

Section 72(1)(b) read with sections 4 and 5, in particular, prescribes that before a cloud computing user or operator processes any personal information, the data subject's consent must be obtained first. Section 72 further provides some reasonable flexibility for cloud computing users. Section 72's provisions allow cloud computing users to transfer personal information outside the Republic, however, the processing must be executed lawfully in terms of the POPI Act.

This flexibility under section 72's provisions makes sense. In line with the Act's purpose, the regulation of the processing of personal information in terms of the POPI Act is inconsonant with the constitutional values of democracy.[842] The Act also provides openness with the need for economic and social progress.[843] The regulations are within the information society framework and require removing unnecessary impediments to the free flow of information, including personal information.[844]

---

[837] Section 72(1)(a)(i) of the Protection of Personal Information Act.
[838] *Ibid*.
[839] *Ibid.*
[840] Section 72(1)(a)(ii) of the Protection of Personal Information Act.
[841] Neethling *et al Neethling on Personality Rights* 407.
[842] The Preamble of the Protection of Personal Information Act.
[843] *Ibid*.
[844] Invitation to submit written submissions on the proposed National Data and Cloud Policy: Government gazette Number 309 (44411) (1 April 2021) http//:www.gpwonline.co.za 3 (Accessed 14 May 2021).

Communication methodologies have shifted dramatically over the past decades. Increased Internet penetration and Internet-focused business models such as online shopping and e-commerce have grown exponentially.[845] The economic and social progress stated in the Preamble calls for the flexibility of cross-border flow of personal information through cloud computing services. Section 72 excludes the prohibition of cross-border transfer of personal information if the transfer is necessary to perform a contract between the data subject and the responsible party.[846] It also excludes implementing pre-contractual measures taken in response to the data subject's request.[847]

The exclusion also applies in terms of section 72(1)(d) if the transfer is necessary for the conclusion or performance of a contract. The exclusion applies provided such a contract is concluded in the interest of the data subject between the responsible party and a third party or if the transfer is for the benefit of the data subject.[848] The responsible party who is a cloud computing user could evade liability in terms of the Act for the unlawful transfer of personal information in terms of section 72(1)(e)(i). This provision applies if it is not reasonably practicable to obtain the data subject's consent to that transfer. It also applies if, in terms section 72(1)(e)(ii), it was reasonably practicable to obtain such consent; the data subject would be likely to give it.

In terms of section 72(2), "binding corporate rules" means personal information processing policies within a group of undertakings. A responsible party or cloud computing operator should strictly adhere to these policies within that group of undertakings. It is the type of strict policies applicable when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country.[849] The phrase "binding corporate rules" is not defined under section 1 of the POPI Act; however, section 72(2)(a) provides its definition. The term

[845] Swales 2016 *South African Mercantile Law Journal* 59.
[846] Section 72(1)(c) of the Protection of Personal Information Act.
[847] *Ibid*.
[848] Section 72(1)(e) of the Protection of Personal Information Act.
[849] Section 72(2)(a) of the Protection of Personal Information Act.

“group of undertakings” is also defined under section 72(2)(b). The Act defines the “group of undertakings” as a controlling undertaking and its controlled undertakings.

It is worth noting that responsible parties who conduct cross-border data processing transactions using cloud computing services are bound to conduct themselves, at minimum, with the requirements contained in the POPI Act.[850] Section 57(1)(d) of the POPI Act requires that the IR’s consent be obtained before sending personal information to a foreign country. It is permissible to process data in and to foreign jurisdictions, but consent will be required. Ideally, it will only be obtained if sent to a country where similar data protection legislation exists.[851]

Section 72(1)(a)’s provisions seem to pose a challenge in the context of cloud computing. Firstly, most cloud computing service providers are not domiciled in the Republic for the IR to audit and verify the cloud computing service provider’s corporate rules. Secondly, corporates do not usually publicise their internal data protection controls. If they do, most of the data subjects might be ignorant of what the policies entail, or there might be no adequate transparency on the side of the responsible party. Thirdly, the extent of the IR’s jurisdictional reach has not been tested yet on cloud computing service providers outside the Republic regarding “binding corporate rules”.

Fourthly the possibility is that the corporate rules only bind to a limited extent. They might fall under section 2(d) of the Act under voluntary measures of protecting personal information. The phrase “adequate level of data protection” as used in the POPI Act leaves a gap. It does not specify the extent of adequateness to have an extensive binding force. The phrase “binding agreements” is also vague. It does not prescribe and explicitly provide the provisions of how agreements should be drafted to give them the adequate force of law in the context of cloud computing.

Section 72(1)(a)(i) further states that the cloud computing service provider or the responsible party must effectively uphold principles for reasonable processing of the information. This section does not prescribe what is “reasonable processing of the

[850] Sections 2,3,57, 69, 72 and chapter 3 of the Protection of Personal Information Act.
[851] Section 72(1)(a)(i) and (ii) of the Protection of Personal Information Act.

information….". To what extent does the unreasonableness come in when processing personal information? This is a gap that will require the statutory interpretation theories to determine the legislator's objective and intention and apply the common law doctrine of reasonableness to execute the POPI Act's purpose.

Section 72 further fails to address the remedies and control measures employed should personal information gets processed within a jurisdiction or corporate that does not have adequate data protection mechanisms. It is also important to note that the POPI Act provisions are mostly binding within the Republic. POPI Act is national legislation that has a binding force in the Republic. It is up to the IR to enforce the Act beyond the Republic's territorial borders by enforcing its powers on data protection breaches emanating outside the Republic. Therefore, it suffices to say that the entire section 72 will be of no use if the IR does not take active steps to enforce it beyond the Republic's borders.

Section 72 read with section 3(1)(a)(ii) fails to properly regulate and leave a gap in the processing of personal information where the responsible party is not domiciled in the Republic. The regulatory gap emanates when cloud computing services are used to "forward" personal information through the Republic. Firstly, it can be argued that forwarding personal information falls under "processing". "Forwarding", in literal terms, is a continuation of a process that has not reached its final "destination",[852] although not explicitly mentioned under the definition of the term "processing" under section 1 or anywhere in the POPI Act.

The term "Forwarding" in the context of cloud computing could fall under "dissemination by means of transmission", as explicitly mentioned under the definition of the term "processing" using automated means. If the mere "forwarding" of personal information through the Republic is excluded from the POPI Act's provisions, therefore responsible parties could evade liability. In the form of a scenario, where the personal information transmitted through the Republic gets breached within the South African territory while being "forwarded", the affected data subject will be forced to rely on

[852] South African Oxford School Dictionary 242.

other forms of seeking remedy other than section 72 and section 3(1)(a)(ii) as the complaint will be falling outside their scope.

"Forwarding" in the cloud computing context will have to use a network to transmit information. It will also require equipment capable of operating automatically in response to the instructions given.[853] This further shows that the "forwarding" of personal information does not happen in an open-ended process. "Forwarding" in this context requires all the elements of automated transmission mentioned in the POPI Act's provisions. In this case, the literal interpretation of the term "forwarding" will lead to absurdity on the Act's purpose.

Section 2(c), read with section 99, provides persons with rights and remedies to protect their personal information from processing that is not according to the Act. Any breach of personal information processed using cloud computing is actionable under the law of delict or damages by enforcing the civil remedies indicated under section 99 of the POPI Act. When this research was conducted, there was no case law available that has been presided over in terms of the POPI Act. The POPI Act is relatively new legislation, with certain sections still not in force yet.

4.10 Civil remedies in terms of the POPI Act

It is necessary to juxtapose the common law defences to vicarious liability with the defences available to the responsible party regarding the POPI Act. A data subject may elect to base their claim against the responsible party on the common law or POPI Act remedies. The doctrine of vicarious liability, in its modern form, is motivated by considerations of public policy.[854] Public policy demands that a person whose rights have been wrongfully infringed upon should not be left without a claim.[855]

A person whose privacy has been infringed upon through the unlawful, culpable processing of their personal information can sue the responsible party. Section 99 provides liability without fault where ordinary common law remedies require at least

[853] Section 3(4) of the Protection of Personal Information Act.
[854] Gabriel 2019 *THRHR* 16.
[855] *Ibid*.

negligence.[856] This effectively gives a data subject whose responsible party has unwittingly fallen foul of the POPI Act's provisions a civil claim with a lower fault threshold than required in terms of the common law.

One vicarious liability area that remains available for deliberation is the statutory vicarious liability in terms of the POPI Act.[857] The provisions of section 99[858] for the civil remedies on unlawful processing of personal information will be discussed below in a cloud computing context.

At the data subject's request, the IR, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of the POPI Act as referred to in section 73.[859] The IR may, on its initiative, decide to launch an investigation into interference with the personal information of a data subject.[860]

Section 99(2) further provides that, in the event of a data breach, the responsible party may raise any defences against an action for damages. The available defences include *Vis major*, consent of the plaintiff and fault on the part of the plaintiff.[861] If compliance was not reasonably practicable in the circumstances of the particular case and if the IR has granted an exemption in terms of section 37, that could also be raised as a defence.[862] To the responsible party's detriment, the POPI Act does not recognise good deeds, intentions, or aspirations as defences to a civil claim brought in section 99.

Section 99(3) provides that a court hearing proceedings in terms of subsection (1) may award a just and equitable amount. Such an award includes payment of damages as

[856] Gabriel 2019 *THRHR* 613.
[857] Statutory vicarious liability is where a statute imposes strict liability on one party for the actions of another; Abraham and Gross Attorneys, Notaries and Conveyances "Vicarious Liability and What It Means for Employers" (14 November 2017) Criminal Law, Labour and Employment Litigation and Dispute Resolution https://www.abgross.co.za/vicarious-liability-and-employers/ (Accessed 25 February 2022).
[858] The date of commencement of section 99 was 1 July 2020.
[859] Section 99(1) of the Protection of Personal Information Act.
[860] Section 76(3) of the Protection of Personal Information Act.
[861] Section 99(2)(a)(b) and (c) of the Protection of Personal Information Act.
[862] Section 99(2)(d) and (e) of the Protection of Personal Information Act.

compensation for patrimonial and non-patrimonial loss suffered by a data subject due to a breach of the provisions of the POPI Act.[863] Section 99(8) provides that any civil action instituted under section 99 may be withdrawn, abandoned or compromised. However, any agreement or compromise must be made an order of the Court.[864] If civil action has not been instituted, any agreement or settlement, if any, may, on application to the Court by the IR after due notice to the other party, be made an order of the Court.[865] The Court's order must then be published in the *Gazette* and by such further public media announcement as the Court considers appropriate.[866]

Based on Section 99(1), the Act does not specify which courts have jurisdiction to preside over the civil action for damages on cloud computing matters. Section 107, read with section 108, does provide such a provision. Section 108 provides that any person convicted of an offence in terms of the POPI Act, Magistrate's court has jurisdiction to impose penalties as provided in section 107.

No clarity is provided on the extent of the Magistrate Court's jurisdiction on international cloud computing data breaches. Debatable so, in section 108, the provision is made that, "…despite anything to the contrary in any other law...", a Magistrate's Court has jurisdiction to impose any penalty provided for in section 107. The phrase "any other law" could be interpreted to mean the laws of the Republic.

The question will be if the data breach or unlawful processing of personal information emanates from another sovereign jurisdiction, would the Magistrate Courts still have the jurisdiction to preside and decide over the case? If the matter is then taken to High Courts, at what stage and under what circumstances will a matter on cloud computing services data breaches fall above the Magistrate Court's scope? The POPI Act is not clear in this regard. The POPI Act is also unclear whether the affected data subject has to report the matter first to the Magistrate's Courts, after that, follow the hierarchy to the Higher Courts through appeal, review or transfer, or data subjects could approach the High Court with jurisdiction directly.

[863] Section 99(3)(1)(a) of the Protection of Personal Information Act.
[864] Section 99(8) of the Protection of Personal Information Act.
[865] Section 99(9) of the Protection of Personal Information Act.
[866] *Ibid*.

Firstly, the POPI Act does not provide the explicit rules to be followed in the conflict of laws. In a scenario where the provisions of the POPI Act clash with the data protection laws of another sovereign state, the POPI Act is silent. The importance of the inclusion of such a provision for cloud computing is because of its cross-border data flows characteristic. Should a data breach materialise in another jurisdiction, then the conflict of laws arise.

Secondly, as mentioned above, most cloud computing service providers are not domiciled in South Africa. Thirdly, cloud computing services can be utilised to process personal information without the responsible party being physically domiciled in the Republic. When such scenarios arise, the IR faces the challenge of determining which courts of which jurisdiction have the authority to preside over the matter and which law is applicable.

Section 99(3) seems to be restricted in the South African context, while sections 107,108 and 109 explicitly address all the penalties and administrative fines in the event of a civil ligation. The provisions of section 99(3), which reads "…may award an amount that is just and equitable", fails to address what is "just" and "equitable". In the South African context, what can be seen as just and equitable might not be "just" and "equitable" in another jurisdiction.

If a data breach occurs in the severs of a cloud computing service provider domiciled in another jurisdiction, how will the IR determine what is just and equitable for the affected data subjects? If the matter is decided on the said jurisdiction, the court will provide what it deems just and equitable in terms of the data protection laws of that country. This will be regardless of whether the quantum is above or below what is considered just and equitable by the IR. The Act does not provide other measures that the IR will employ to challenge the court's decision in another jurisdiction if the amount awarded is deemed not just and equitable.

The main objective of systems and guidelines that enforces data protection mechanisms is to deliver a good level of compliance.[867] These enforcement mechanisms support data subjects in exercising their right to privacy by appropriately redressing the injured party where such rights have been violated.[868]

4.11 Penalties and administrative fines for non-compliance with the POPI Act

Penalties for non-compliance with the provisions of the POPI Act are, on the face of it, severe. Chapter 11 of the POPI Act deals with offences, penalties and administrative fines. In section 107, the maximum penalty is 10 years in prison or an administrative fine of RI0 million. The Regulator can provide remedial mechanisms for non-compliance with the provisions of the POPI Act, but the nature and scope of infringements are entirely clarified in chapter 7 and sections 60 to 68.

Section 107[869] provides that any person convicted of an offence in terms of the POPI Act is liable, in the case of an infringement of section 100, 103 (1), 104 (2), 105 (1), 106 (1), (3) or (4). The conviction could range from a fine or imprisonment for a period not exceeding 10 years or to both a fine and such imprisonment.[870] The infringement of sections 59, 101, 102, 103 (2) or 104 (1) could lead to a fine or imprisonment for a period not exceeding 12 months or both a fine and such imprisonment.[871]

Offences under the POPI Act are dealt with in sections 100 to 106. They include the breach of the duty to treat confidential personal information that comes to the responsible party's knowledge. Failure by a responsible party or cloud computing service provider to comply with an enforcement notice renders the responsible party liable for damages. Failure by a responsible party or cloud computing service provider to comply with lawful processing conditions related to personal details of a data subject also renders the responsible party liable.

[867] Neethling *et al Neethling on Personality Rights* 407.
[868] *Ibid* and Roos 2006 *CILSA* 234 to 235.
[869] The date of commencement of section 107 was 1 July 2020.
[870] Section 107(1)(a) of the Protection of Personal Information Act.
[871] Section 107(1)(b) of the Protection of Personal Information Act.

Without the consent of the responsible party, a third party knowingly discloses or procures the disclosure of personal information of a data subject to another person also renders the third party liable. Liability also arises where a third party unlawfully sells or offers to sell the personal information of a data subject. Conviction of any of these offences renders one liable to a fine or imprisonment not exceeding 10 years or both.[872]

Both the Magistrate's Court and the High Court have jurisdiction to impose any penalties specified in the Act.[873] Suppose it is alleged that a responsible party has committed an offence in terms of the POPI Act, in that case, the IR may cause an infringement notice to be served on the responsible party (the infringer).[874] The infringer may choose to pay or make arrangements to pay the fine.[875] The infringer may also elect to be tried in court on a charge of having committed an offence.[876] In this case, the IR must hand the matter over to the South African Police Services (SAPS).[877] Administrative fines may not exceed R10 million.[878]

Section 107(1) states that any person convicted of an offence in terms of the POPI Act is liable for an infringement of certain POPI Act sections. The phrase "any person" could be interpreted as including natural (private) persons as well. Specifically, the contravention of sections 69, 71 and 72 of the POPI Act are not explicitly mentioned under section 107 as punishable. The Act is not clear as to what kind of penalties are attached to them specifically. This then raises the question of what criteria the IR will use to address sections 69, 71, and 72 as far as penalties are concerned. The regulations are also silent in this regard.

4.12 Other obstacles of the POPI Act

[872] Section 107(a) and (b) of the Protection of Personal Information Act.
[873] Section 108 of the Protection of Personal Information Act.
[874] Section 109(1) of the Protection of Personal Information Act.
[875] Section 109(2)(d)(i) and (ii) of the Protection of Personal Information Act.
[876] Section 109(2)(d)(iii) of the Protection of Personal Information Act.
[877] Section 109 (1) to (3) of the Protection of Personal Information Act.
[878] Section 109(2)(c) of the Protection of Personal Information Act.

One of the issues raised by practitioners and mooted by parties affected by the POPI Act was whether the POPI Act applies retrospectively.[879] The concern was that immediately before POPI Act coming into force, a surge of personal information would have been transferred in a final attempt to compile precious databases for marketing and business purposes.[880] The collected personal information would be processed and kept in the cloud computing servers for a long time. Such processing is regarded as unlawful processing as consent from the data subjects is not initially obtained.

It seems like POPI Act does not apply retrospectively in its current form. This position will still stand in the absence of the POPI Act being amended or the President bringing other parts of it into force with retrospective effect.[881] The POPI Act would be too large a burden to administer and enforce retrospectively. Under section 69 of the POPI Act, the consent and opt-out provisions would provide data subjects with sufficient ability to curtail the processing of their personal information on cloud computing services relatively quickly.[882]

Section 72's provisions affect South African businesses' ability to transfer information in the global marketplace. It does, however, allow South African companies to receive data flow from countries that have similar data protection provisions in their jurisdiction. Had POPI Act not been drafted with a limitation on trans-border data flows, South African businesses would struggle to transact with companies based in the EU. In cases where South African companies wish to engage trans-border data flows to countries with lower data protection standards than South Africa, obtaining the data subject's consent or satisfying another exception to section 72's prohibitions would ease restrictions on South African businesses from engaging in transborder data flows to companies in those jurisdictions.[883]

[879] R Luck "Is South Africa Keeping Up with International Trends?" (22 May 2013) *De Rebus* http://www.saflii.org/za/journals/DEREBUS/2014/84.pdf (Accessed 12 March 2020).
[880] *Ibid.*
[881] *Ibid*.
[882] R Luck "POPI- Is South Africa Keeping Up with International Trends?" (1 May 2014) *De Rebus* http://www.derebus.org.za/popi-south-africa-keeping-international-trends/ (Accessed 12 March 2020).
[883] *Ibid*.

4.13 Conclusion

The POPI Act makes provisions and conditions for the lawful processing of personal information. The Act's provisions provide "adequate" data protection standards to secure SA's participation in the international trade market.[884] Because cloud computing involves massive cross-border data flows, the POPI Act provides provision for personal information across SA borders. There is a need for SA's POPI Act to comply with the data protection standards of the GDPR to remain part of the international information technology market.[885] The arising concern is whether the POPI Act meets the minimum standard of data protection set out by the GDPR or whether the revision of certain provisions of the POPI Act is needed.

[884] Neethling *et al Neethling on Personality Rights* 414 and Naude and Papadopoulos (2) 2016 *THRHR* 229.
[885] Neethling *et al Neethling on Personality Rights* 414.

Chapter 5: A comparative study of the Protection of Personal Information Act 4 of 2013 and the European Union's General Data Protection Regulation

5.1 Introduction

The GDPR is an EU data protection legislation approved by the European Union Parliament in April 2016 with a two-year buffer period before its provisions became effective on 25 May 2018.[886] The Regulation replaces the 1995 Data Protection Directive.[887] It aims to give consumers control of their data processed by companies. The GDPR affects organisations within the EU, but it also applies to companies outside of the EU region if they offer goods or services to or monitor the behaviour of data subjects in the EU.[888] The GDPR regulates two types of data handlers: "controllers" and "processors." It protects identified or identifiable natural persons referred to as "data subjects".

Like the POPI Act, the GDPR does not explicitly address cloud computing as the only form of personal data processing. It is important to analyse and interpret certain provisions and terms of the GDPR to determine if it addresses cloud computing services or not. This chapter will follow a comparative study of the GDPR and the POPI Act on certain selected provisions. This section will analyse the provisions on establishing the Supervisory Authorities under the GDPR, their functions, powers and scope. It will further analyse the GDPR's provisions on cross-border transfer of personal data, the remedies and penalties for the breach of the GDPR's provisions. The last part of the chapter will provide the concluding remarks.

5.2 How does the GDPR affect the POPI Act?

When the SALRC brought out its report on data protection legislation for South Africa, it recommended that South Africa adopt legislation that met the international standards

[886] GDPR FAQs: Frequently Asked Questions About GDPR https://eugdpr.org/the-regulation/gdpr-faqs/ https://perma.cc/3WBX-EEE4 *EU GDPR.ORG* (Accessed 07 August 2021).
[887] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals concerning the Processing of Personal Data and the Free Movement of Such Data [1995] OJ L281/31.
[888] GDPR FAQs: Frequently Asked Questions About GDPR.

for data protection, of which they recommended the EU Directive.[889] The Directive that the POPI Act was built upon, was later replaced by the GDPR.

The Directive affected countries outside the EU, such as SA, because Article 25 required third-world countries to provide adequate data protection before sending personal data from EU countries to third countries. The GDPR has a similar requirement under Article 44 to that of the Directive, and, as a result, third countries have to ensure that they provide a level of data protection that meets the GDPR standard.[890] POPI Act has a similar provision under section 72.

If the POPI Act meets the standards set out on cloud computing data protection and privacy, the EU Commission have to declare the POPI Act's data protection adequacy. If the Commission makes such a finding, subsequent transfers of personal data from the EU to South Africa through cloud computing services will be possible without employing appropriate safeguards or binding corporate rules.[891]

5.3 Purpose of the GDPR

The purpose of the GDPR is threefold.[892] Firstly, the stated objectives of the GDPR consists of strengthening personal data protection efforts and unifying European data protection law.[893] Secondly, the GDPR seeks to instil confidence in citizens of the EU member countries by ensuring their private data will be protected by those organisations that seek to use it.[894] The GDPR explicitly grants new rights for EU citizens regarding their data.[895] Thirdly, the EU sought to boost Europe's digital

[889] South African Law Reform Commission *Privacy and Data Protection* 109 para 3.2.7. and Roos 2020 *Comparative and International Law Journal of Southern Africa* 4.
[890] Article 44 of the General Data Protection Regulation.
[891] Roos 2020 *Comparative and International Law Journal of Southern Africa* 6.
[892] G Carlson, J McKinney, E Slezak and E S Wilmot "General Data Protection Regulation and California Consumer Privacy Act: Background" (2020) 24 *Currents Journal of International Economic Law* 62 and M Rosentau "The General Data Protection Regulation and Its Violation of EU Treaties" (2018) 27 *JURIDICA INT'l* 36 at 38.
[893] A von dem Bussche-Freiherr and A Zeiter "Implementing the EU General Data Protection Regulation: A Business Perspective" (2016) 2 *European Data Protection Law Review* 576 and Carlson 2020 *Currents Journal of International Economic Law* 62.
[894] Carlson 2020 *Currents Journal of International Economic Law* 63 and Rosentau 2018 *JURIDICA INT'l* 36.
[895] Carlson 2020 *Currents Journal of International Economic Law* 63.

economy through these new protections.[896] Carlson believes that if people felt that their data was handled securely, they would be more willing to use digital services.[897]

The provisions contained in the GDPR lay down rules relating to the protection of natural persons concerning the processing of their data by the controllers[898] using cloud computing services.[899] It is worth noting that instead of the term "responsible party" as used in the POPI Act, the GDPR preferred the term "controller".[900] Instead of the term "personal information" used in the POPI Act, the GDPR preferred "personal data".[901] The terms "controller" and "personal data" will be analysed below in a cloud computing context. However, the terms do not have different connotations as used in both legislations.

The GDPR provides rules relating to the free movement of personal data as cloud computing services involve massive cross-border data flows.[902] This is a similar provision provided by the South African POPI Act under Section 2(a)(ii). The free movement of personal data within the EU shall be neither restricted nor prohibited in the GDPR.[903] This entails that the movement of personal data within the EU through cloud computing services is not prohibited, provided that the processing of such personal data complies with the conditions of the GDPR.

The GDPR also aims to protect natural persons' fundamental rights and freedoms and their right to protection of personal data using cloud computing services.[904] The

---

[896] *Ibid*.
[897] *Ibid*.
[898] Article 4(1) and (8) of the General Data Protection Regulation, Opinion 1/2010 on the concepts of "controller" and "processor", Article 29 Working Party, WP 169, 00264/10/EN, Brussels,16 February 2010 at 4 and L Oprysk "The Forthcoming General Data Protection Regulation in the EU" (2016) 24 *JURIDICA INT'l* 23 at 25 and Rosentau 2018 *JURIDICA INT'l* 38.
[899] S M Puiszis "Unlocking the EU General Data Protection Regulation" (2018) *J. PROF.LAW.* 1 at 3 and Article 4 (7) of the General Data Protection Regulation defines a "controller" as a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
[900] Article 4(7) of the General Data Protection Regulation.
[901] Article 4(1) of the General Data Protection Regulation.
[902] Article 1(1) and 44 of the General Data Protection Regulation.
[903] Article 1(3) of the General Data Protection Regulation.
[904] Article 1(2) of the General Data Protection Regulation and A Schildhaus "EU's General Data Protection Regulation GDPR: Key Provisions and Best Practices" (2017) 46 *INT'l L. News* 12, I Alexe

protection of natural persons concerning the processing of personal data is a fundamental right recognised by the GDPR.[905] Article 8(1) of the Charter of Fundamental Rights of the European Union[906] and Article 16(1) of the Treaty of the Functioning of the European Union (TFEU) also recognise personal data as a fundamental right.[907] These two pieces of legislation provide that everyone has the right to protect personal data concerning them.[908]

The regional treaties and agreements have to abide by the GDPR to protect data and the right to privacy. There has been a significant debate on the GDPR's violation of the EU treaties.[909] In other words, in essence, the GDPR runs counter to the "constitutional organisation" of the EU, formed in line with the establishing treaties as the GDPR is, at the base, a "European law" that applies to all the EU Member States.[910] In essence, the GDPR is not a treaty, and it cannot be classified as a regional agreement or convention; instead, it is the EU Law that is binding and enforceable on all the EU subjects.

When the legislation's purpose has been established, it is crucial to understand its scope and employ proper regulatory interpretation methodologies to apply its provisions properly on a case-by-case basis. In the following paragraphs, the scope of the GDPR will be analysed in the cloud computing context.

"The Sanctioning Regime Provided by Regulation (EU) 2016/679 on the Protection of Personal Data" (2018) *INT'L LAW REVIEW* 60 at 61 and W G Voss and H Bouthinon-Dumas "EU General Data Protection Regulation Sanctions in Theory and Practice" (2020) 37 *Santa CLARA HIGH TECH. L. J*. 1 at 7.

[905] J Dumas "General Data Protection Regulation (GDPR): Prioritizing Resources" (2019) 42 *Seattle U. L. REV.* 1115 at 1116, Puiszis 2018 *J. PROF. LAW.* 2 and Schildhaus 2017 *INT'l L. News* 12.

[906] Charter of Fundamental Rights of the European Union 2012/C 326/02 (Charter of Fundamental Rights of the European Union, Preamble: The Union is founded on the indivisible and universal values of human dignity, freedom, equality and solidarity; this is based on the principles of democracy and the rule of law. The Union places the person at the heart of its action, establishing the citizenship of the Union and creating an area of freedom, security and justice.) and A Cormack "Incident Response: Protecting Individual Rights under the General Data Protection Regulation" (2016) 13 *SCRIPTed* 258 at 260.

[907] The Charter of Fundamental Rights of the European Union provides for Article 7; One of the freedoms considered fundamental, namely Respect for private and family life. At the same time, Article 8 establishes another fundamental right, namely the protection of personal data and D Manescu "Recovery of Claims in the GDPR (General Data Protection Regulation) Era" (2018) 8 *JURIDICAL TRIB* 789 at 790, Rosentau 2018 *JURIDICA INT'l* 36 and Cormack 2016 *SCRIPTed* 260.

[908] Roos 2020 *Comparative and International Law Journal of Southern Africa* 2.

[909] Rosentau 2018 *JURIDICA INT'l* 36.

[910] *Ibid*.

5.4 The scope of the GDPR

The GDPR applies to process personal data in the context of establishing a controller in the EU.[911] The material scope of the GDPR applies to the processing of personal data wholly or partly by automated means.[912] The term "automated means" is not defined under Article 4 of the GDPR, defining specific terms. The term is also not defined anywhere in the GDPR. However, the closest term defined under Article 4 with a more relative link to the term "automated means" is "profiling", which will be discussed below in a cloud computing context.

The scope of the GDPR further applies to any processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[913] A similar provision is articulated in the POPI Act.[914] The GDPR provides penalties for non-compliance by controllers with the GDPR, which are potentially significant. These penalties can range up to £20 million or 4% of an entity's annual worldwide turnover of severe violations.[915]

The GDPR provides explicit provisions for its objective and its scope as far as personal data processing is concerned in the context of cloud computing. The following discussion is on how the GDPR applies to the processing of personal data by controllers within and outside the EU using cloud computing services.

5.5 Application and interpretation of the GDPR

Article 94 of the GDPR provides the Repeal of Directive 95/46/EC by the GDPR. The Directive was repealed with effect from 25 May 2018.[916] It is important to note that the

---

[911] W G Voss "Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation" (2016) 50 *R.J.T. n.s.* 783 at 798.
[912] Article 2(1) of the General Data Protection Regulation.
[913] *Ibid*.
[914] Section 3(1)(a) of the Protection of Personal Information Act.
[915] Articles 83(2) to (6) of the General Data Protection Regulation lists a series of factors to be considered by a supervisory authority in determining whether to impose an administrative fine and, if so, the amount of that fine and Puiszis 2018 *J. PROF.LAW.* 2.
[916] Article 94(1) of the General Data Protection Regulation, S Bhaimia "The General Data Protection Regulation: the Next Generation of EU Data Protection" (2018) 18 *LIM* 21, G Spindler and P Schmechel "Personal Data and Encryption in the European General Data Protection Regulation" (2016) 7 *J. INTELL. PROP. INFO. TECH. & ELEC. COM. L.* 163 at 164, Von dem Bussche Freiherr 2016 *European*

references to the repealed Directive shall be construed as references to the GDPR.[917] References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive is construed as references to the European Data Protection Board (EDPB) established by the GDPR.[918] Article 99 states that the GDPR applied from 25 May 2018.[919]

5.5.1 Interpretation of the GDPR

It is essential to highlight that as much as the GDPR provides for the application of its provisions, it does not provide its interpretation. When interpreting an article of the GDPR, recitals to the GDPR must also be taken into account to interpret the article.[920] The Court of Justice of the European Union (CJEU) answered questions from national courts of Member States on the interpretation of the GDPR and the Directive. This is so because the same rule may continue in the GDPR from the Directive on cloud computing services. CJEU decisions on the interpretation of the Directive in the context of cloud computing and the right to privacy remain relevant.[921]

Advocate Generals of the CJEU submit non-binding opinions for some cases to the courts. Even where the CJEU has not followed the opinion before, it provides essential background to the decision.[922]

5.5.2 Territorial Scope for the application of the GDPR

On the application of the GDPR, Article 95 outlines the relationship of the GDPR and the Directive on the applicability of the data protection provisions. The GDPR does not impose additional obligations on natural or legal persons. This is in relation to

---

Data Protection Law Review 576, Carlson 2020 *Currents Journal of International Economic Law* 62 and Schildhaus 2017 *INT'l L. News* 12.

[917] Article 94(2) of the General Data Protection Regulation, Bhaimia 2018 *LIM* 21, Spindler 2016 *J. INTELL. PROP. INFO. TECH. & ELEC. COM. L.* 164 and Von dem Bussche Freiherr 2016 *European Data Protection Law Review* 576.

[918] Article 94(2) of the General Data Protection Regulation and Bhaimia 2018 *LIM* 21.

[919] Article 99(2) of the General Data Protection Regulation, Bhaimia 2018 *LIM* 21, Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 576 and A S Perrin "The General Data Protection Regulation and Open Source Software Communities" (2021) 12 *Cybaris INTELL. PROP. L. REV.* 77 at 78.

[920] Bhaimia 2018 *LIM* 21.

[921] Bhaimia 2018 *LIM* 22.

[922] *Ibid*.

processing in connection with publicly available electronic communications services in public communication networks in the EU. These are electronic communications such as the ones concerning matters for which they are subject to specific obligations with the same objective set out in the Directive.[923]

The GDPR is binding and directly applicable in all Member States of the EU.[924] The GDPR has a general application and passes into law without further action by the EU Member States.[925] It ensures uniform application across the EU region and has little or no room for flexibility for the Member States to "tweak" the GDPR's provisions and transport them into national legislation.[926] National law will still be required, even if only to enact the national derogations in the GDPR and to repeal or amend national law implementing the GDPR.[927]

International agreements involving the transfer of personal data to third countries or international organisations concluded by the Member States before 24 May 2016 and complied with EU law as applicable before the enforcement date remains in force until amended, replaced or revoked.[928]

The GDPR applies whether the use of cloud computing services to process personal data takes place in the EU's territorial borders or not.[929] This jurisdictional application

[923] Article 95 of the General Data Protection Regulation.
[924] Article 99(2) of the General Data Protection Regulation, E O'Dell "Compensation for the Breach of the General Data Protection Regulation" (2017) 40 *DUBLIN U. L.J.*97 at 102, Bhaimia 2018 *LIM* 21, Spindler 2016 *J. INTELL. PROP. INFO. TECH. & ELEC. COM. L.*164, Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 576, Carlson 2020 *Currents Journal of International Economic Law* 62, Schildhaus 2017 *INT'l L. News* 12, Rosentau 2018 *JURIDICA INT'l* 38 and Voss 2020 *Santa CLARA HIGH TECH. L. J.* 7.
[925] F Gilbert "Proposed EU Data Protection Regulation: The Good, the Bad and the Unknown" (2012) 15(10) *Journal of Internet Law* 1 at 22 to 23, Roos 2020 *Comparative and International Law Journal of Southern Africa* 3, Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 576, Schildhaus 2017 *INT'l L. News* 12, Rosentau 2018 *JURIDICA INT'l* 38 and Voss 2020 *Santa CLARA HIGH TECH. L. J.* 7.
[926] Roos 2020 *Comparative and International Law Journal of Southern Africa* 3 and Schildhaus 2017 *INT'l L. News*12.
[927] Bhaimia 2018 *LIM* 21 and Rosentau 2018 *JURIDICA INT'l* 38.
[928] Article 96 of the General Data Protection Regulation.
[929] Article 3(1) of the General Data Protection Regulation, Puiszis 2018 *J. PROF. LAW.* 2, Spindler 2016 *J. INTELL. PROP. INFO. TECH. & ELEC. COM. L.*164, Perrin 2021 *Cybaris INTELL. PROP. L. REV.* 78, Schildhaus 2017 *INT'l L. News* 12 and Manescu 2018 *JURIDICAL TRIB*. 790.

is based upon a controller's presence in the EU.[930] Where the controller is a public or a private body or a cloud computing service provider is established in the EU, not only will the GDPR apply to such processing activities, there must be a trigger such as processing personal data or a data breach to activate the application of the GDPR. This is regardless of the location of those activities.

Such activities should relate to offering goods or services such as Amazon online services,[931] this is irrespective of whether a payment of the data subject is required to such data subjects in the EU.[932] The provisions also apply for monitoring their behaviour as far as their behaviour takes place within the EU.[933] This extraterritorial scope means overseas companies (particularly internet and technology companies, who were in mind when this rule was added) may find themselves caught by its laws.[934]

The GDPR also applies to third countries and provide provisions for processing personal data using cloud computing services for EU citizens. The controllers in third countries have to ensure that they provide data protection that meets the GDPR standard.[935] According to Article 44 of the GDPR, a transfer of personal data to a third country,[936] if the data is to undergo processing after the transfer, it may take place only if the controller[937] comply with the conditions for processing laid down in the GDPR. The cross-border transfer of personal information will be discussed below.

Article 3(3) further provides that the GDPR applies to the processing of personal data by a controller not established in the EU but in a place where Member State law applies under public international law.

---

[930] Puiszis 2018 *J. PROF.LAW.* 5, Schildhaus 2017 *INT'l L. News* 12 and Manescu 2018 *JURIDICAL TRIB.* 790.
[931] Schildhaus 2017 *INT'l L. News* 12.
[932] Article 3(2)(a) of the General Data Protection Regulation, Puiszis 2018 *J. PROF.LAW*. 2, Spindler 2016 *J. INTELL. PROP. INFO. TECH. & ELEC. COM. L.*164, Carlson 2020 *Currents Journal of International Economic Law* 62 and Schildhaus 2017 *INT'l L. News* 12.
[933] Article 3(2)(b) of the General Data Protection Regulation.
[934] Bhaimia 2018 *LIM* 24.
[935] Roos 2020 *Comparative and International Law Journal of Southern Africa* 5.
[936] Article (44) of the General Data Protection Regulation and Roos 2020 *Comparative and International Law Journal of Southern Africa* 5.
[937] Article 4 (8) of the General Data Protection Regulation defines a "processor" as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

5.5.3 Factors considered to qualify as an establishment in the EU when processing personal data

It is important to note that to be established in the EU or to qualify as an establishment requires the exercise of any real and effective activity, even a minimal one through stable arrangements.[938] Whether through a branch or a subsidiary with a legal personality, the legal form of any such arrangement is not the determining factor.[939] The EDPB issued Guidelines explaining that in some circumstances, the presence of a single employee or an agent in the EU may be sufficient to constitute a stable arrangement.[940] Therefore, the GDPR will apply.

Thus, companies headquartered outside of the EU, without an establishment there, may be subject to the GDPR, so long as they are processing personal data of a data subject in the EU. Provided the processing is connected with the offering of goods or services to them, or monitoring their behaviour, insofar as such behaviour occurs in the EU, they may have to appoint a representative in the EU in terms of the GDPR.

Firstly, the type or size of the business, the number of employees, the nature of the goods or services offered, or the entity's sector makes no difference.[941] Secondly, monitoring their (controller or cloud computing service providers) behaviour as far as their behaviour occurs within the EU is vital for the GDPR to apply.[942] Monitoring behaviour can include online tracking and data processing activities that profile individuals, their behaviours or attitudes or analyse or predict their preferences.[943]

For instance, the mere ability to access a website in the EU is not sufficient to trigger the application of the GDPR.[944] Factors that can trigger the GDPR's application include using a top-level EU domain extension website. This should consist of offering goods or services in a Member State's native language, pricing goods or services in

[938] Puiszis 2018 *J. PROF. LAW.* 5.
[939] *Ibid*.
[940] *Ibid*.
[941] Puiszis 2018 *J. PROF. LAW.* 2 and Spindler 2016 *J. INTELL. PROP. INFO. TECH. & ELEC. COM. L.*164.
[942] Article 3(2)(b) of the General Data Protection Regulation, Spindler 2016 *J. INTELL. PROP. INFO. TECH. & ELEC. COM. L.*164 and Schildhaus 2017 *INT'l L. News* 12.
[943] Puiszis 2018 *J. PROF. LAW*. 6, Spindler 2016 *J. INTELL. PROP. INFO. TECH. & ELEC. COM. L*. 164 and Schildhaus 2017 *INT'l L. News* 12.
[944] Puiszis 2018 *J. PROF. LAW*. 6.

the currency used in that Member State, or the reference to other customers in a Member State.[945]

All these examples mentioned above could trigger the application of the GDPR for online activities. The use of cloud computing services will undoubtedly be covered as one of the online triggers for the GDPR's application. Most companies that offer online services nowadays, such as Amazon online and Google, use cloud computing platforms to provide services. If any of the platforms that use cloud computing services are used to process personal data in and outside the EU, such activity will undoubtedly trigger the application of the GDPR.

The GDPR provides a broader scope and enforceability beyond the territorial borders of the EU. This entails that the GDPR has set a precedent for an "adequate" international data protection standard. Specific provisions and terms used in the GDPR need to be interpreted in a cloud computing context to determine its objective and purpose. These terms are also found in the POPI Act and provide a similar definition as the GDPR. Since these are two different legislations, a discussion of these terms and their application to cloud computing services must be done in the context of the GDPR provisions.

5.6 Interpretation of specific terms

A requirement for a finding of adequate data protection in legislation is that certain basic data protection concepts and principles, such as "personal data", "processing", "controller", "filing system", and "profiling" should exist in the third country's legal system.[946] These concepts and terms do not have to be identical to those of the GDPR but must be consistent.[947] The meaning of these terms as used in the GDPR will be analysed and interpreted in a cloud computing context.

[945] *Ibid*.
[946] Roos 2020 *Comparative and International Law Journal of Southern Africa* 8 and Bhaimia 2018 *LIM* 24.
[947] Roos 2020 *Comparative and International Law Journal of Southern Africa* 8.

The GDPR aims to protect natural persons with regard to the processing of personal data and provide rules relating to the free movement of personal data. There must be a natural living person for the GDPR to apply. If the data subject is deceased or is an existing juristic person, the provisions of the GDPR do not apply.[948] Therefore, the GDPR's protection does not apply to the processing of data concerning legal persons.[949] In particular, undertakings established as legal persons, including the name and the form of the legal person and the legal person's contact details, also fall outside the scope of the GDPR.[950]

The POPI Act provides for similar provisions on protecting the processing of personal information of natural persons.[951] However, the POPI Act extends its protection to juristic persons as well. The extension of personal data protection to juristic persons implies that they also have the right to privacy. However, the rights of natural persons are prioritised over the rights of juristic persons.[952]

5.6.1 The meaning of "personal data"

The GDPR defines "personal data" as any data relating to an identified or identifiable natural person ("data subject").[953] The term "data subject" as frequently used in the GDPR is not defined anywhere. In terms of the GDPR, an identifiable natural person can be identified directly or indirectly by reference to an identifier.[954] The GDPR provides extensive examples of data that can serve as an identifier. Such identifiers could include a name, an identification number, location data or an online identifier.[955]

It could also be one or more factors specific to that natural person's physical, physiological, genetic, mental, economic, cultural or social identity. The POPI Act also provides a similar definition under section 1 for the term "personal information". The POPI Act also provide an extensive list of examples of personal information. The list

[948] Puiszis 2018 *J. PROF.LAW.* 7 and Spindler 2016 *J. INTELL. PROP. INFO. TECH. & ELEC. COM. L.* 164.
[949] Puiszis 2018 *J. PROF.LAW.* 7.
[950] *Ibid*.
[951] The Preamble, section 2 and section 3 of the Protection of Personal Information Act.
[952] Section 1 of the Protection of Personal Information Act.
[953] Article 4(1) of the General Data Protection Regulation.
[954] *Ibid* and Carlson 2020 *Currents Journal of International Economic Law* 64.
[955] *Ibid*.

is not closed, and other information may be regarded as personal information if it relates to a person who is identifiable from that information. The list includes information that can be considered specific to the "physical, physiological, genetic, mental, economic, cultural or social identity" of that data subject, as mentioned in the GDPR.[956]

With such a striking similarity in the definition of personal information, it can be noted that POPI Act is adequate on data protection based on the international data protection standard set by the GDPR. The fact that the POPI Act also recognises that juristic persons may in certain circumstances be entitled to personality rights, specifically the right to a good name and privacy[957] explains why juristic persons are included in the definition under the POPI Act. However, this does not detract from the minimum standard set by the GDPR. In fact, the scope of the POPI Act is broader than that of the GDPR.[958]

The GDPR provides a broader scope of examples for the definition of "personal data", which is broken down into different categories. Article 4(13) further extends the meaning of "personal data" and refer to it as "generic data", and provide for its definition exclusively. Such generic data must still be attached to a natural living person for the provisions of the GDPR to apply. The term "genetic data" means personal data relating to a natural person's inherited or acquired genetic characteristics.[959] These characteristics must give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.[960]

On the other hand, Article 4(14) extend the meaning of "personal data" to encamps "biometric data" concerning a natural person. The term "biometric data" means personal data resulting from specific technical processing relating to a natural person's

[956] Roos 2020 *Comparative and International Law Journal of Southern Africa* 9.
[957] Neethling *et al Neethling's Law of Delict* 342 to 345 and Roos 2020 *Comparative and International Law Journal of Southern Africa* 9.
[958] Roos 2020 *Comparative and International Law Journal of Southern Africa* 9.
[959] Article 4(13) of the General Data Protection Regulation.
[960] *Ibid*.

physical, physiological or behavioural characteristics.[961] These characteristics must allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.[962]

The provisions of Article 4(15) defines "data concerning health" of a natural person. Such processing must refer to personal data relating to a natural person's physical or mental health. These include the provision of health care services, which reveal information about the health status of the data subject concerned. Therefore, the "data concerning health" falls under the broader definition of "personal data".

Though relating to a natural person, processing specific personal data can be excluded from the definition of "personal data", such data is referred to as "sensitive personal data". The definition of sensitive personal data under the GDPR includes criminal convictions and offences or related security measures.[963] However, the processing of criminal information can only occur under the control of official authority or authorised by EU or Member State law that provides appropriate safeguards for the rights and freedoms of the data subjects.[964]

Personal data that falls under the term "pseudonymisation"[965] also falls outside the scope of the GDPR.[966] Anonymising personal data requires personal data to be processed to no longer be attributed to a specific person without additional information. Regarding the POPI Act, "pseudonymisation" is personal data that has been de-identified to the extent that it cannot be re-identified again.[967]

"Pseudonymisation" is possible if the additional information is kept separate and protected by the cloud computing service provider's technical measures to ensure the

[961] Article 4(14) of the General Data Protection Regulation.
[962] *Ibid*.
[963] Article 9 and 10 of the General Data Production Regulation.
[964] Article 10 of the General Data Production Regulation.
[965] Article 4(5) of the General Data Production Regulation; provides that "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
[966] Puiszis 2018 *J. PROF. LAW*. 7.
[967] Section 6(1)(a) and (b) of the Protection of Personal Information Act.

personal data cannot be attributed to any specific person.[968] Anonymization of data can satisfy the GDPR's obligation to consider privacy by design and default.[969] Encrypted data plays a significant role in protecting data subjects' privacy.[970] Its legal problems are closely related to the scope of the data protection laws and the legal effects of anonymisation and pseudonymisation.[971]

When a controller processes personal data, the natural person to whom the information relates must provide consent[972] first and in that mode, they are referred to as "data subject".[973] The GDPR provides the principles that the controller must comply with before, during, and after processing personal data.[974] On the other hand, the GDPR provides the data subjects with the right to process their data.[975] The POPI Act also echoes similar provisions.[976] The term data subject is discussed below in the context of cloud computing.

5.6.2 The meaning of "data subject"

Though the term "data subject" is not explicitly defined anywhere in the GDPR, its frequent use makes it a vital term to be discussed in a cloud computing context. The term is closely linked to the term "natural person", as indicated under Article 4(1) of the GDPR, which defines the term "personal data". The "data subject" is the identified or identifiable individual to whom the personal data relates. The individual can be an employee, a business contact at a client or a consumer.[977] The reference to data subjects in the GDPR extends to EU citizens and residents and potentially anyone in the EU.[978] The presence of the data subject in the EU is a crucial consideration. A person's nationality or citizenship is irrelevant.

---

[968] Puiszis 2018 *J. PROF. LAW*. 7.
[969] Article 25(1) and (2) of the General Data Protection Regulation and Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 577.
[970] Spindler 2016 *J. INTELL. PROP. INFO. TECH. & ELEC. COM. L.*163.
[971] *Ibid*.
[972] Article 1(11) defines the term "consent" as the consent of the data subject freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by explicit affirmative action, signifies agreement to the processing of personal data relating to them.
[973] Article 4(1) of the General Data Protection Regulation.
[974] Chapter II of the General Data Protection Regulation.
[975] Chapter III of the General Data Protection Regulation.
[976] Chapter 3 and section 5 of the Protection of Personal Information Act.
[977] Article 4(1) of the General Data Protection Regulation and Bhaimia 2018 *LIM* 23.
[978] Guidelines 3/2018 at 13 and Puiszis 2018 *J. PROF. LAW.* 6.

The presence in the EU alone is not enough; a targeting activity directed to the data subjects in the EU is also a requirement.[979] This entails that if the controller using cloud computing services or the service provider itself is breached, such a breach is presumed to have targeted the data subject. This is so because it is the information of the data subject that has been compromised. Therefore, there must be a targeting activity directed to the data subject, which is within the EU territory regardless of their citizenship status, for the GDPR provisions to apply. Such a requirement that the data subject is present in the EU is accessed when the targeting activity occurs.[980]

The components and characteristics of cloud computing services can allow a data breach to occur anywhere in the world. Firstly, the perpetrator does not have to be physically present in the country that has been breached. The second aspect is that the data subject does not have to be physically located in the same country where the cloud computing servers are. Analysing the provisions of the GDPR in this context makes sense that as long as the data subject is within the EU, the provisions of the GDPR will apply regardless of where the targeting activity materialised. This provision explicitly addresses cloud computing and clearly articulates the purpose and intention of the GDPR, which is protecting unlawful processing of personal data of natural persons in the EU.

5.6.2.1 Rights of the data subject

The GDPR provides several rights to data subjects concerning their data and corresponding obligations on controllers to meet and comply with those rights.[981] These rights include the right to learn whether a controller is processing a person's data.[982] The data subject must know the purposes for that processing, the categories of personal data involved and any recipients or categories of recipients with whom the

[979] Puiszis 2018 *J. PROF. LAW.* 6.
[980] *Ibid*.
[981] Articles 13 and 23 of the General Data Protection Regulation, Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 579 and Schildhaus 2017 *IN'l L. News* 12.
[982] Article 12 of the General Data Protection Regulation, Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 579 and Schildhaus 2017 *INT'l L. News* 12.

data will be shared.[983] The period that information will be stored must also be communicated to the data subject.[984] This makes sense as cloud computing services can store information for a prolonged period. Additionally, a data subject has the right to request that a controller correct or delete any personal data desired by the data subject.[985]

The data subject also has a right to object to processing their data or restrict its processing.[986] Controllers will have to take action upon request by any data subject without undue delay, no later than one month after receiving the request.[987] It is the duty of the controller and the cloud computing service provider to protect personal data in their possession.[988] The data subject must learn of automated decision-making or profiling by a controller.[989] They also have a right to receive meaningful information about the logic involved in automated decision-making processes.[990]

The POPI Act provides similar provisions under section 5 on the data subject's rights. However, the POPI Act falls short of offering a provision for the concept of data portability. The concept of data portability is one of the most important novelties in the GDPR in terms of warranting control rights.[991] The data subjects in the EU enjoy the benefits of data portability, meaning that they can order that their data is transferred

[983] Article 15 of the General Data Protection Regulation, Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 579, Carlson 2020 *Currents Journal of International Economic Law* 64 and Schildhaus 2017 *INT'l L. News* 12.
[984] Article 15(1)(d) of the General Data Protection Regulation, Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 579, Carlson 2020 *Currents Journal of International Economic Law* 64, Schildhaus 2017 *INT'l L. News* 12 and Manescu 2018 *JURIDICAL TRIB.* 792.
[985] Article 16 and 17 of the General Data Protection Regulation, Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 579, Carlson 2020 *Currents Journal of International Economic Law* 64 and Schildhaus 2017 *INT'l L. News* 12.
[986] Article 18 of the General Data Protection Regulation, Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 579, Carlson 2020 *Currents Journal of International Economic Law* 64 and Schildhaus 2017 *INT'l L. News* 12.
[987] Article 12 (3) of the General Data Protection Regulation and Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 579.
[988] Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 579 and Carlson 2020 *Currents Journal of International Economic Law* 64.
[989] Article 21 and 22 of the General Data Protection Regulation.
[990] Article 15(1)(h) of the General Data Protection Regulation.
[991] Article 20 of the General Data Protection Regulation and Yav 2018 *International Journal Data Protection Officer, Privacy Officer and Privacy Counsel* 20.

from a controller or service provider to another.[992] This is a matter which POPI Act does not address.[993]

While timely complying with data subject access requests may sound simple on paper. Given the complexity of cloud computing services involving multiple locations where data may be stored and accessed around the globe, compliance has proven to be complex, challenging, and time-consuming.[994] It is essential to analyse the term "processing" in a cloud computing context. For such personal data to reach specific multiple locations around the globe, certain activities must have been engaged into using cloud computing services to process that personal data.

5.6.3 The meaning of "processing"

The term "processing" is defined by the GDPR as any operation or set of operations performed on personal data or sets of personal data in this context using cloud computing services.[995] Such processing, whether or not it's done by automated means such as computers, servers, and databases, falls within the scope of "processing".[996] "Processing" also applies to the manual processing of personal data as part of a filing system or when intended to form part of a filing system.[997] Thus, the GDPR applies to paper and other tangible records containing personal data in a filing system.

Other forms such as collection, recording, organisation, structuring, storage, adaptation or alteration also fall within the scope of "processing".[998] The GDPR regards the retrieval, consultation, use, and disclosure by transmission as "processing". Dissemination of personal data falls within the scope of the GDPR as the processing of personal data.[999] Making available, alignment or combination, restriction and the final stage of handling personal data such as erasure or destruction

[992] Article 20(2) of the General Data Protection Regulation.
[993] Yav 2018 *International Journal Data Protection Officer, Privacy Officer and Privacy Counsel* 20.
[994] Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 579 and Carlson 2020 *Currents Journal of International Economic Law* 64.
[995] Article 4(2) of the General Data Protection Regulation and Manescu 2018 *JURIDICAL TRIB*. 789.
[996] *Ibid*.
[997] *Ibid*.
[998] *Ibid*.
[999] *Ibid*.

are regarded as “processing” in the GDPR.[1000] The South African POPI Act also provides a similar definition for “processing” under section 1.

The definition of the term “processing” under the POPI Act is more than adequate to meet the data protection standards set by the GDPR.[1001] The definition appears to be even more comprehensive than that of the GDPR. It includes operations performed on data and covers processing activities concerning data.[1002] Roos argues that “any activity concerning personal information” and “any operation performed on personal information” arguably amounts to the same thing.[1003] However, Roos concludes that the bottom line is that both the POPI Act and the GDPR define processing in broad terms, and processing essentially includes anything that can be done with personal data.[1004]

As interpreted in the previous chapter, the processing of personal data using cloud computing platforms is addressed under the GDPR as per the term “processing” definition on both legislations. Though not explicitly stated in the GDPR, the GDPR intends to regulate any form of personal data processing, which involves using computer networks and transmission mechanisms, including cloud computing services.

For the processing of personal data to occur, there must be another party who determines the purpose of processing such personal data. The GDPR imposes requirements upon data “processors” and “controllers,” so it is important to understand how each is defined. The obligations imposed by the GDPR differ for processors and controllers. In this context, the term “controller” will be analysed extensively in a cloud computing context.

The “processor” is merely a natural or legal person, public authority, agency or other body which processes personal data using cloud computing platforms on behalf of the

[1000] *Ibid*.
[1001] Roos 2020 *Comparative and International Law Journal of Southern Africa* 10.
[1002] *Ibid*.
[1003] *Ibid*.
[1004] *Ibid*.

controller.[1005] This means that the "controller" remains the "mastermind" behind the processing of such personal data. Accordingly, assigning the data processor role to a cloud computing service provider has been questioned and debated under the EU data protection. Nonetheless, the Article 29 Working Party[1006] declared that a cloud computing service provider becomes a data processor by providing the data controller with the means and platform for processing personal data.[1007]

5.6.4 The meaning of "controller"

In terms of Article 4(7) of the GDPR, the term "controller" is defined as a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data using cloud computing platforms.[1008] The provisions of the GDPR expressly and explicitly extend its scope and jurisdiction to natural persons as well in their capacity as "controllers". This definition immediately includes personal data processing by private individuals using cloud computing services within the GDPR scope.

It is, however, not clear in terms of the GDPR how the penalties and administrative fines will be applied to private persons for contravening the GDPR provisions. Penalties and administration fines under Articles 83 and 84 might be too harsh for a private individual to bear for unlawfully processing personal data using cloud computing services.[1009]

[1005] Article 4(8) of the General Data Protection Regulation and Carlson 2020 *Currents Journal of International Economic Law* 64.

[1006] The Article 29 Working Party was set up in accordance with Article 29 of the Data Protection Directive to provide, *inter alia,* advice on uniform application of the Data Protection Directive and Oprysk 2016 *JURIDICA INT'l* 26.

[1007] Opinion 05/2012 on Cloud Computing, Working Party, WP 196, 01037/12/EN 2012 at 4 and Oprysk 2016 *JURIDICA INT'l* 26.

[1008] Carlson 2020 *Currents Journal of International Economic Law* 64.

[1009] Article 83 of the General Data Protection Regulation provides that each Supervisory Authority shall ensure that the imposition of administrative fines pursuant to the Regulation in respect of its infringements referred to in paragraphs 4, 5 and 6 shall in each case be effective, proportionate and dissuasive. In contrast, Article 84 of the General Data Protection Regulation states that the Member States shall lay down the rules on other penalties applicable to infringements of the Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

The purposes and means of such processing are determined by EU or Member State law. The controller or the specific criteria for its nomination may be provided by EU or Member State law.[1010] Depending on the circumstances, the same entity can be a controller and a processor with respect to its various processing activities.

On the other hand, the POPI Act defines the term "responsible party", similar to the term "controller" under section 1 of the POPI Act. However, the POPI Act's definition of the term "operator" stipulates that the processing must be done in terms of a mandate or other contract with the responsible party, without the operator coming under the direct authority of the responsible party.[1011]

5.6.4.1 Principles for the lawful processing of personal data

This study section will not provide an extensive analysis of the GDPR's principles for the lawful processing of personal data. The time and space allocated for this research are very minimal to cover all the concepts and provisions of the GDPR. However, to archive the purpose and scope of this research, the seven principles for the lawful processing of personal data will be discussed briefly. The discussion will also be necessary as the processing of personal data by the controllers can only be done lawfully if they comply with these principles.

The GDPR requires a cloud computing user or controller to have at least one lawful basis for processing EU data subjects' personal data. Some of the basis could include the data subject's consent and processing necessary for the performance of a contract.[1012] Compliance with a legal obligation is also a lawful basis for processing personal data using cloud computing services.[1013] A legitimate interest pursued by the controller, or when necessary to protect the data subject's vital interests of another natural person, one lawful basis for the processing is established in that context.[1014]

[1010] Article 26 of the General Data Protection Regulation.
[1011] Roos 2020 *Comparative and International Law Journal of Southern Africa* 11.
[1012] Article 6 and 24 of the General Data Protection Regulation and Schildhaus 2017 *INT'l L. News* 13.
[1013] Article 5(2) of the General Data Protection Regulation and Carlson 2020 *Currents Journal of International Economic Law* 64.
[1014] Article 6 of the General Data Protection Regulation The processing of special categories of sensitive personal data falls under the ambit of Article 9 General Data Protection Regulation. The processing of personal data relating to criminal convictions, offences, and related security measures is governed by Article 10 General Data Protection Regulation.

This obligation requires that a controller review all of its data processing activities and confirm a lawful basis for each such activity.[1015]

Personal data can only be processed on the cloud computing servers for specific, explicit and legitimate purposes.[1016] Information collected for one purpose cannot be used or processed for purposes other than the one processed for in the servers.[1017] Additionally, data controllers must demonstrate compliance with these principles as outlined by the GDPR.[1018] The GDPR emphasises record keeping and documentation to demonstrate compliance with its requirements.[1019] Records must be kept of all processing activities, including the lawful grounds for any processing activity.[1020]

Cloud computing users must ensure lawfulness, fairness, and transparency.[1021] The controller must ensure that any information and communication relating to the processing of personal data must be easily accessible, easy to understand, and presented using clear and plain language.[1022]

"Lawful" processing falls into five different categories such as consent, contract, legal obligations, public policy or public interest. Legitimate interests that do not override the interests or fundamental rights of the data subject also constitute lawful processing of personal data in a cloud computing context.[1023] To process lawfully means finding a lawful ground and not breaching other laws, including the Article 8 right to privacy in the European Convention on Human Rights 4.XI.1950, Rome.[1024]

[1015] Article 5(1)(a) and Chapter IV of the Data Protection Regulation and Schildhaus 2017 *INT'l L. News* 12.
[1016] Article 5(1)(b) and 6(1)(a) of the General Data Protection Regulation.
[1017] Article 5(1)(b) of the General Data Protection Regulation.
[1018] Article 5(2) of the General Data Protection Regulation.
[1019] Article 30 of the General Data Protection Regulation.
[1020] *Ibid*.
[1021] Article 5(1)(a) of the General Data Protection Regulation.
[1022] Article 7(2) of the General Data Protection Regulation.
[1023] Article 6(1)(a) to (f) of the General Data Protection Regulation.
[1024] Bhaimia 2018 *LIM* 25.

There must be a purpose limitation on the processing of personal data by a controller or cloud computing service provider.[1025] Data may only be used for the specific purpose identified by the controller. Data minimisation is a vital component when processing personal data under the GDPR [1026] This means that data collected must be relevant and limited to what is necessary for the purposes for which it is processed.[1027] The controller should not further collect additional data relevant to the processing needed unless there is a legitimate purpose determined at the time of the data collection. Data minimisation is a crucial aspect of the GDPR's "data protection by default and design".[1028] Article 25 requires controllers to consider data protection at the design stage of projects and products, not at the end.[1029]

Accuracy of personal data must be ensured during the processing of personal data by the controller and the cloud computing service provider.[1030] Personal data must be accurate and kept current. Where data is inaccurate, it must be remedied and rectified without delay. [1031] The term accuracy in this context includes the right to be forgotten.[1032] Data subjects have a right to compel controllers or cloud computing service providers to erase their data and stop third parties from processing the data.

Article 17 of the GDPR provides for a data subject's right to have information about him or herself erased from the cloud computing servers. The right to be forgotten was first recognised in a landmark case, namely, *Google Spain SL v AEPD (the DPA) and Maria Costeja Gonzalez.*[1033] In this case, an individual brought a complaint against Google, claiming that the information retrieved by a search engine relating to a debt that had since been paid was no longer relevant or favourable. The court held that the

[1025] Article 5(1)(b) of the General Data Protection Regulation, Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 580 and Carlson 2020 *Currents Journal of International Economic Law* 64.
[1026] Article 5(1)(c) of the General Data Protection Regulation.
[1027] *Ibid* and Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 580.
[1028] Article 25 of the General Data Protection Regulation.
[1029] Bhaimia 2018 *LIM* 25.
[1030] Article 5(1)(d) of the General Data Protection Regulation and Carlson 2020 *Currents Journal of International Economic Law* 64.
[1031] Article 5(1)(d) and Article 16 of the General Data Protection Regulation, Bhaimia 2018 *LIM* 26 and Carlson 2020 *Currents Journal of International Economic Law* 64.
[1032] Article 17 of the General Data Protection Regulation, Bhaimia 2018 *LIM* 26, Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 579 and Schildhaus 2017 *INT'l L. News* 13.
[1033] (2014) C-131/12, 13.5.

search engine operator must erase information and links in the search results list, although not from the Internet entirely.[1034] This case is relevant to cloud computing services as the Google platform uses cloud computing platforms to provide its services, and cloud computing can also store data for a prolonged period.

The case of *GC et al v CNIL*[1035] concerns four individuals who requested that Google stop showing in its search results links to websites containing articles or content that third parties had published about them. Specifically, the search results in question led users to a satirical photomontage of a local politician; to an article that described one of the individuals as a Church of Scientology public relations officer. It also linked them to a judicial investigation of business people and political personalities; and, finally, to an article about a criminal conviction for the sexual assault of minors.

Google refused to comply with their requests, arguing that the personal data of the four individuals, although sensitive, were essential to the public interest and should therefore remain available to online users. After the French data protection authority (CNIL) upheld Google's decision, the applicants brought the case to the French council of state (Conseil d'Etat), which referred a list of concrete questions to the CJEU on the provisions of the GDPR.[1036]

The controller has an obligation concerning the storage limitation of personal data processed in cloud computing service provider servers.[1037] The storage of personal data should be limited to the purposes for which the personal data was processed.[1038]

Controllers and cloud computing service providers should take measures to ensure the storage of personal data held in backups or servers is aligned to the stated

[1034] Gabriel 2019 *THRHR* 612.
[1035] (2019) C-136/17 para 71 to 79.
[1036] E Pirkova and E Masser "The EU Court decides on two major "right to be forgotten" cases: there are no winners here" (23 October 2019) *Access now* https://www.accessnow.org/eu-court-decides-on-two-major-right-to-be-forgotten-cases-there-are-no-winners-here/ (Accessed 09 August 2021).
[1037] Article 5(1)(e) of the General Data Protection Regulation and Carlson 2020 *Currents Journal of International Economic Law* 64.
[1038] Article 5(1)(e), (f) and Article 25 of the General Data Protection Regulation.

purpose.[1039] This principle addresses the use of cloud computing services to process personal data. The controller has to choose a processor who, in this context, is a cloud computing services provider that provides sufficient guarantees regarding the technical security and organisational measures governing data processing and must ensure that processor's compliance.[1040]

An extension of storage limitation could also be the integrity and confidentiality (security), which must be in place upon processing personal data.[1041] Both the controllers and cloud computing service providers must take explicit steps to prevent unauthorised access to personal data and the equipment used for processing personal data.[1042] To enforce security, controllers and cloud computing service providers must provide clear notice of data collection, outline processing purposes and use cases, and define their data retention and deletion policies.[1043]

There must be a legally binding contract between the controller and processor (cloud computing service provider). In the contracts, the obligation to ensure appropriate technical and organisational measures to protect the data must also be binding for the processor.[1044] The obligation to conclude a binding agreement serves to provide the data controller with complete control over the processing of personal data and eases ensuring data protection compliance.[1045]

Cloud computing service providers supply their services based on terms of service[1046] specified on a Web page. These agreements, in most cases, are decided upon unilaterally, especially with public IaaS. They do not assure that the service to be delivered suits the client's purposes.[1047] While large enterprises might have the

[1039] *Ibid*.
[1040] Articles 17 (2), 28(1) and 23 of the General Data Protection Regulation and Oprysk 2016 *JURIDICA INT'l* 26.
[1041] Article 5(1)(f) of the General Data Protection Regulation and Cormack 2016 *SCRIPTed* 267.
[1042] Articles 5(1)(e), 28(1) and 32 of the General Data Protection Regulation.
[1043] Articles 5(1)(e), 24, 25 and 28(1) of the General Data Protection Regulation.
[1044] Articles 28(3) and 32 of the General Data Protection Regulation and Oprysk 2016 *JURIDICA INT'l* 26.
[1045] Oprysk 2016 *JURIDICA INT'l* 26.
[1046] *Ibid*.
[1047] *Ibid*.

bargaining power to negotiate a tailored contract as IaaS clients, the same certainly is not true for Small and Medium Enterprises (SMEs).[1048]

The controller and the cloud computing service providers have to establish and maintain a process to identify a breach in a timely manner.[1049] They should also understand why it occurred, who was affected and notify affected data subjects.[1050] Breach notifications are, therefore, vital. The notice to the affected data subjects must be given within seventy-two hours of a data breach when the breach might compromise the data subject's privacy.[1051]

In terms of Article 5, accountability is a requirement for the lawful processing of personal data.[1052] The controller is responsible for demonstrating compliance with the above requirements. Some examples include the creation and ability to demonstrate new policies, processes, and training.[1053] There must be evidence of valid consents given by data subjects[1054] and detailed data record keeping.[1055] A Data Protection Officer (DPO) appointment is also vital to monitor accountability.[1056]

The above principles echo those of its predecessor, the Directive. However, the GDPR carries with it additional features that raise the stakes. It has a long reach and applies to any controller doing business with EU citizens.[1057] It specifies fines of up to 4% annual worldwide turnover or E20 million (whichever is greater) in the event of a

---

[1048] *Ibid*.
[1049] Article 32 of the General Data Protection Regulation and Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 578.
[1050] Article 33 of the General Data Protection, Von dem Bussche Freiherr 2016 *European Data Protection Law Review* 578 and Cormack 2016 *SCRIPTed* 263.
[1051] Article 33(1) of the General Data Protection Regulation and Von dem Bussche Freiherr 2016 *European Data Protection Law Review* 578, Schildhaus 2017 *INT'l L. News* 13 and Cormack 2016 *SCRIPTed* 263.
[1052] Article 5(2) of the General Data Protection Regulation, Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 579 to 580, Carlson 2020 *Currents Journal of International Economic Law* 63 and Carlson 2020 *Currents Journal of International Economic Law* 64.
[1053] Article 24 of the General Data Protection Regulation and Carlson 2020 *Currents Journal of International Economic Law* 63.
[1054] Article 6(1)(a) and 7(2) of the General Data Protection Regulation and Carlson 2020 *Currents Journal of International Economic Law* 164.
[1055] Article 30 of the General Data Protection Regulation and Carlson 2020 *Currents Journal of International Economic Law* 164.
[1056] Article 37 of the General Data Protection Regulation and Carlson 2020 *Currents Journal of International Economic Law* 164.
[1057] Article 3(2) of the General Data Protection Regulation.

breach.[1058] Within hours of the GDPR taking effect on May 25, 2018, companies like Google, Facebook, Instagram, and WhatsApp that also use cloud computing services received privacy complaints that could carry fines of up to $9.3 billion in total.[1059]

The GDPR also applies to the processing other than by automated means of personal data, which form part of a filing system or are intended to form part of a filing system. However, cloud computing services fall within the term "automated means" surprisingly; the GDPR does not provide its definition. The term "automated means" only appears under Article 4 (4) on the definition of the term "profiling". The term profiling is discussed below in a cloud computing context.

5.6.5 Interpretation of the term "profiling"

In terms of the GDPR, "profiling" means any form of automated processing of personal data consisting of personal data to evaluate certain personal aspects relating to a natural person.[1060] In particular, analysing or predicting aspects of a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements fall within the scope of "profiling".[1061] Section 71[1062] of the POPI Act makes provisions for "automated decision making",

[1058] Article 83(5) to (6*)* of the General Data Protection Regulation.
[1059] S Keane "GDPR: Google and Facebook Face up to $9.3B in Fines on the First Day of New Privacy Law" (25 May 2018) *CNET* https://www.cnet.com/news/gdpr-google-and-facebook-faceup-to-9-3-billion-in-fines-on-first-day-of-new-privacy-law (Accessed 02 July 2021) and Dumas 2019 *Seattle U. L. REV.* 1119.
[1060] Article 4(4) of the General Data Protection Regulation.
[1061] *Ibid*.
[1062] Automated decision making.—(1) Subject to subsection (2), a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including their performance at work, or his, her or its creditworthiness, reliability, location, health, personal preferences or conduct.
(2) The provisions of subsection (1) do not apply if the decision—
(*a*) has been taken in connection with the conclusion or execution of a contract, and—
(i) the request of the data subject in terms of the contract has been met; or
(ii) appropriate measures have been taken to protect the data subject's legitimate interests; or
(*b*) is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.
(3) The appropriate measures, referred to in subsection (2) (a) (ii), must—
(*a*) provide an opportunity for a data subject to make representations about a decision referred to in subsection (1); and
(*b*) require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations in terms of paragraph (a).

which has a similar intention as the definition of the term “profiling” under the GDPR on data protection.

The POPI Act, as discussed above, also has the same intention as the GDPR, to regulate “automated means” and “non-automated means”. The GDPR, however, does not provide such an extended definition as the POPI Act does.

If such processing falls under non-automated means as provided for under Article2(1), the use of cloud computing will still be within the scope of the GDPR.[1063] Its application will depend on whether the recorded personal data is processed by non-automated means to form part of a filing system or intended to form part. Therefore, interpreting the term “filing system” in relation to cloud computing services becomes necessary.

5.6.6 The meaning of a “filing system”

Article 4 (6) defines the term “filing system” as any structured set of personal data accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.[1064] A cloud computing server, cabinet or hard drive containing Human Resources (HR) records of employees with their names or other identifiers is an example of a relevant filing system. However, documents maintained by year only and not organised by name or arranged by some other identifier do not qualify as a filing system under the GDPR. Data contained in documents within such a server would fall outside the scope of the GDPR until it is structured or organised with some unique identifiers.[1065]

The POPI Act has a similar definition under section 1 of the term “filing system”, which means that the POPI Act is adequate for data protection. A similar interpretation of the term “filing system” employed in the previous chapter under the POPI Act also applies to the GDPR.

[1063] Mashinini 2020 *De Jure Law Journal* 154.
[1064] Article 4(6) of the General Data Protection Regulation.
[1065] Puiszis 2018 *J. PROF. LAW.* 9.

However, the GDPR has included a list of activities excluded from the meaning of personal data.[1066] The GDPR provides for exclusion, exemption and exception from the purposes of the GDPR certain processing activities from its provisions. Exclusions, exemptions and exceptions are allowed where processing only poses a small risk to the data subject's privacy or where overriding interests of other persons have to be taken into account.

5.7. Exclusion and exception of certain personal data processing

Firstly, the GDPR prohibits processing special categories of personal data, namely data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Such data include genetic data, biometric data to uniquely identify a natural person, data concerning health or a natural person's sex life or sexual orientation.[1067]

In terms of Article 2(2), the GDPR does not apply to the processing of personal data in the course of an activity that falls outside the EU law scope.[1068] The GDPR also does not apply if the Member States' processing of personal data when carrying out activities that fall within the scope of chapter 2 of title V of the Treaty of the European Union (TEU).[1069]

Most importantly, the GDPR will not apply if a natural person does the processing in the course of a purely personal or household activity.[1070] The exemption seems to apply to natural persons, not juristic persons using cloud computing services. It is worth noting that the term "controller" encompasses the natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of processing personal data. In this context, natural persons are not recognised as "controllers" provided they use cloud computing services to process

[1066] Article 2(2) of the General Data Protection Regulation.
[1067] Article 9(1) of the General Data Protection Regulation Particular categories of personal information are treated as "sensitive" information because it is assumed that the misuse of these types of information could have more severe consequences for a data subject's fundamental rights and Roos 2020 *Comparative and International Law Journal of Southern Africa* 12.
[1068] Article 2(2)(a) of the General Data Protection Regulation.
[1069] Article 2(2)(b) of the General Data Protection Regulation.
[1070] Article 2(2)(c) of the General Data Protection Regulation.

personal data for personal or household activities. The POPI Act contains a similar provision in section 6 as analysed above.[1071]

"Household purposes" exemption in terms of the GDPR applies to personal record-keeping, correspondence, and personal social networking activities. Processing that is partly personal and partly business or professional, such as sending emails or letters that include social and business-related content, does not fit within this exemption. Social networking providers also do not fall within this exemption.[1072]

Guidance as to the scope of the household exception as provided for in terms of the GDPR is found in Article 29 of the Data Protection Working Party's Opinion on online social networking.[1073] The opinion provides that where access to profile information extends beyond self-selected contacts, such as when access to a profile is provided to all members within the social network, where the data is indexable by search engines, or if the user takes an informed decision to extend access beyond self-selected friends, such access goes beyond the household sphere, and the household exception would not apply.

This issue was considered by the CJEU in *Bodil Lindqvist v Åklagarkammaren i Jönköping* [1074] and *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy.*[1075] It recommended that a criterion be inserted to differentiate between personal and non-personal processing based on whether data is disseminated to a finite or indefinite number of individuals.[1076]

The term "personal or household activities" is not defined anywhere in the GDPR. Drawing a line between what is and what is not purely personal household activity for EU data subjects may be difficult in some instances. For instance, since the provision excludes the natural persons, how will the provisions apply if the natural person

[1071] Section 6(1)(a) and (b) of the Protection of Personal Information Act.
[1072] Puiszis 2018 *J. PROF. LAW*. 6.
[1073] Gabriel 2019 *THRHR* 608.
[1074] (2003) C-101/01.
[1075] (2008) C-73/07.
[1076] Gabriel 2019 *THRHR* 608.

processes personal data for commercial activities online but within the framework of "personal or household activities". The GDPR is not precise in this context.

If competent authorities do the processing for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and preventing threats to public security, the GDPR will not apply.[1077] Based on the above analysis, the provisions of the POPI Act are essentially equivalent to those in the GDPR.[1078]

To promote, protect, and fulfil the GDPR's objectives and clarify its application of certain provisions, the GDPR provides for establishing Supervisory Authorities (SA). The SA has to exercise certain powers and perform specific duties and functions in terms of the GDPR. The meaning and the scope of the SAs will be discussed in the paragraphs below.

5.8 Establishment of independent supervisory authorities

Each Member State is required to provide one or more independent public authorities to act as a Supervisory Authority (SA)[1079] under the GDPR. Each SA shall act with complete independence in performing its tasks and exercising its powers in accordance with the GDPR.[1080] The member or members of each SA shall, in the performance of their tasks and exercise of their powers in accordance with the GDPR, remain free from external influence, whether direct or indirect.[1081] The SAs shall neither seek nor take instructions from anybody.[1082]

Each SA is considered competent to perform the tasks required under the GDPR. These tasks include monitoring and enforcing GDPR compliance by promoting public

[1077] Article 2(2)(d) of the General Data Protection Regulation.
[1078] Roos 2020 *Comparative and International Law Journal of Southern Africa* 12.
[1079] Article 51(1) of the General Data Protection Regulation.
[1080] Article 52(1) of the General Data Protection Regulation, M Szydfo "The Independence of Data Protection Authorities in EU Law: Between the Safeguarding of Fundamental Rights and Ensuring the Integrity of the Internal Market" (2017) 41 *European Law Review* 369 and O'Dell 2017 *DUBLIN U. L.J.* 100.
[1081] Article 52(2) of the General Data Protection Regulation.
[1082] *Ibid*.

awareness of risks, rules, and safeguards concerning personal data.[1083] The SAs must also promote controllers' and processors' awareness of their obligations under the GDPR when using cloud computing services to process personal data.[1084] The SAs can archive this by conducting investigations into potential violations,[1085] handling complaints of data subjects or their representatives[1086] as well as establishing requirements for data impact assessments.[1087]

The SA must adopt standard contractual clauses and approve binding corporate rules of data controllers.[1088] Encouraging and approving the development of codes of conduct, certification mechanisms, seals, and marks also fall within the scope of the SA.[1089] SAs are further granted the power to perform data protection audits[1090] and to order controllers, processors, and, where applicable, their representatives to provide information and access to personal data or premises when necessary to perform its tasks.[1091] In this context, the phrase "…and, where applicable, their representatives…" could be interpreted to include cloud computing service providers as "processors".

The GDPR further require the SAs to issue warnings about likely violations of personal data[1092] and to issue reprimands for violations of personal data.[1093] To order processing activities to be brought into compliance with the GDPR and order a controller to make a breach notification to data subjects for such a breach must be enforced by the SAs.[1094] The SAs should further impose limitations, including a complete ban on processing activities by the controller or cloud computing service provider to unlawful processing of personal data or inadequate data protection mechanisms.[1095]

[1083] Article 52(4) of the General Data Protection Regulation.
[1084] Article 57(1) of the General Data Protection Regulation.
[1085] Article 57 (1)(h) of the General Data Protection Regulation.
[1086] Article 57 (1)(f) of the General Data Protection Regulation.
[1087] Article 57 (1)(k) of the General Data Protection Regulation.
[1088] Article 57 (1)(j) of the General Data Protection Regulation.
[1089] Article 57 (1)(m)(n) and (o) of the General Data Protection Regulation.
[1090] Article 58 (1)(b) of the General Data Protection Regulation.
[1091] Article 58 (1)(d)(e)(f) of the General Data Protection Regulation.
[1092] Article 58 (2)(a) of the General Data Protection Regulation.
[1093] Article 58 (2)(b) of the General Data Protection Regulation.
[1094] Article 58 (2)(c)(d) and (e) of the General Data Protection Regulation.
[1095] Article 58 (2)(f) of the General Data Protection Regulation.

After an investigation has been conducted and concluded, the SA can impose administrative fines for violating the right to privacy and unlawful processing of personal data.[1096] If the unlawfulness involved cross-border data flows through cloud computing services, the SA can order the suspension of data flows outside the EU.[1097]

The exercise of these powers is subject to judicial review and due process following EU or Member State law.[1098] Member State law may grant additional powers to SAs, including the right to bring legal actions to enforce the GDPR.[1099] Identifying a lead SA should be established when a controller established in the EU carries out processing activities in the multiple Member States, such as cloud computing service providers.[1100]

The lead SA will be where the controller's main establishment is located, where the major personal data processing decisions are made.[1101] The SA will then regulate controllers across all EU Member States. For example, where a South African business has one or more offices in the EU, it may identify where its main establishment is located in the EU to avoid dealing with multiple SAs.

While the concept of appointing a DPO is adopted in the EU, it also has been adopted in the South African data protection law, the POPI Act. Under the GDPR, however, controllers and cloud computing service providers must designate a DPO. Such designation will be based on their "core activities" consisting of processing operations that involve the "regular and systematic" monitoring of data subjects on a "large scale" such as online behavioural tracking or "large scale" processing of special categories of "sensitive" personal data.[1102]

[1096] Article 58 (2)(i) of the General Data Protection Regulation.
[1097] Article 58(2)(j) of the General Data Protection Regulation.
[1098] Article 57(4) of the General Data Protection Regulation.
[1099] Article 58(5)(6) of the General Data Protection Regulation.
[1100] Article 56 of the General Data Protection Regulation.
[1101] Article 4(16) of the General Data Protection Regulation.
[1102] Article 37(1)(a), (b) of the General Data Protection Regulation (A DPO is also required when processing is carried out by a public authority or public body, "except for courts acting in their judicial capacity".

A controller or processor's "core activities" relate to its primary activities and not the processing of data as ancillary activities. However, the GDPR does not attempt to define what constitutes "large scale processing" or what qualifies as "regular and systematic" monitoring of data subjects in the EU. The DPOs remain subject to the SAs in terms of the GDPR.

Under the South African POPI Act, section 39 establishes the IR as an independent supervisory body. The IR has authoritative powers in the Republic as a single body, while the GDPR requires each Member State to provide more than one SA under certain circumstances.[1103] The EU SAs can also work jointly with other SAs from the different Member States. In a nutshell, the scope, competence, powers and the tasks of both the IR in terms of the POPI Act and the SAs in terms of the GDPR are similar. Therefore, the POPI Act provides adequate data protection measures that meet the international data protection benchmark.

The GDPR has set the minimum standard for any other jurisdiction wishing to exchange personal data with the EU Member States to meet data protection standards. The POPI Act does regulate the trans-border flows of personal data to countries without adequate data privacy protection laws; under section 72.[1104] The typical standard for allowing data transfer is an adequate level of data protection in the receiving country. However, there are exceptions, such as contracts and consent of the data subject.[1105] The GDPR makes the cross-border transfer of personal data provisions under chapter V of the GDPR. A detailed discussion of chapter V in the context of cloud computing is provided below.

5.9 Transfers of personal data to third countries and international organisations

Article 4(23) of the GDPR defines the term "cross-border processing". The term means processing personal data in the context of the activities of establishments in more than

[1103] Article 51(1) of the General Data Protection Regulation.
[1104] Neethling *et al Neethling on Personality Rights* 406.
[1105] *Ibid.*

one Member State of a controller in the EU. The controller must be established in more than one Member State for the GDPR to apply.[1106]

The term "cross-border processing" also means processing personal data in the context of the activities of a single establishment of a controller or processor in the EU. The processing must substantially affect or likely affect data subjects significantly in more than one Member State.[1107] This provision regulates the use of cloud computing to process personal data. Personal data can easily be moved across multiple jurisdictions in a short space of time through cloud computing services. This means cloud computing is likely to substantially affect data subjects in more than one Member State in the EU, triggering the GDPR application.

The GDPR impacts international flows of personal data and, therefore, cross-border trade in services.[1108] Chapter V of the GDPR provides provisions for transferring personal data outside the European Economic Area (EEA).[1109] The EU stands out for its commitment to the sui generis protection of personal data as a fundamental right, which stretches beyond the fundamental right to privacy.[1110] The export of personal data from within and outside the EU to third countries is subject to formalities that aim to provide safety of personal data so that it cannot be rendered meaningless by the transfer of personal data to so-called "data havens".[1111] Personal data originating from the EEA's data subjects can be transferred without further safeguards pursuant to a formal finding from the EU of an adequate level of protection in the receiving country, often called an "adequacy finding".

In terms of the GDPR, personal data cannot be transferred through cloud computing services to third countries or international organisations outside the EU unless the GDPR's requirements are met.[1112] These include the conditions for onward transfer of

[1106] Article 45 of the General Data Protection Regulation.
[1107] Article 4(23) (b) of the General Data Protection Regulation.
[1108] S Yakovleva and K Irion "Toward Compatibility of EU Trade Policy with the General Data Protection Regulation" (2020) 114 *AJIL UNBOUND* 10.
[1109] The EEA extends the EU internal market by three European Free Trade Association states Iceland, Liechtenstein, and Norway.
[1110] Yakovleva 2020 *AJIL UNBOUND* 10.
[1111] *Ibid*.
[1112] Article 44 of the General Data Protection Regulation.

personal data from the third country to another third country. Any transfer to a third country may be carried out only in full compliance with the GDPR.[1113] The level of protection for the personal data mandated by the GDPR cannot be undermined by the transfer of that data to a country outside the EU[1114]

According to the GDPR, personal data may be transferred to a third country based on an adequacy decision,[1115] or subject to appropriate safeguards,[1116] which may include binding corporate rules.[1117] Irrespective of how the transfer takes place, the crux is that personal data must enjoy adequate protection in the third country. Section 72(1)(a) of the POPI Act provides a similar provision.

Transfers of personal data are permitted to a country or an international organisation[1118] that the European Commission has determined provides an adequate level of protection to personal data an "adequacy decision".[1119] Such a transfer using cloud computing services shall not require any specific authorisation.[1120]

The GDPR also permits the Commission to make adequacy determinations for countries and specific territories or sectors within a country. [1121] Adequacy determinations must be reviewed every four years,[1122] and the Commission is charged with monitoring ongoing developments in each approved country that could affect adequacy determination. [1123] Transfers of personal data to countries that have

[1113] This means that the third country must also prohibit the further transfer of personal data from that country to another third country that does not provide adequate data protection and Roos 2020 *Comparative and International Law Journal of Southern Africa* 5.
[1114] Article 44 of the General Data Protection Regulation.
[1115] Article 45 of the General Data Protection Regulation.
[1116] Article 46 of the General Data Protection Regulation.
[1117] Article 47 of the General Data Protection Regulation.
[1118] Article 4 (26) states that "international organization" means an organisation and its subordinate bodies governed by public international law or any other body set up by, or based on, an agreement between two or more countries.
[1119] Article 45(1) of the General Data Protection Regulation (Countries that have previously been approved are: Andorra, Argentina, Canada (where the PIPEDA is applicable), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Uruguay, and New Zealand.
[1120] Article 45(1) of the General Data Protection Regulation.
[1121] Article 45(3) of the General Data Protection Regulation.
[1122] *Ibid*.
[1123] Article 45(4) of the General Data Protection Regulation.

received an adequacy determination do not otherwise require any specific approval or authorisation.[1124]

In assessing the adequacy of the protection provided by a third country, the Commission must take some aspects into account.[1125] Such elements include the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence and effective functioning of one or more independent SAs.[1126] The Commission should also consider the international commitments the third country or international organisation has entered into.[1127] In the absence of an adequacy decision, personal data transfer may occur if the controller has provided appropriate safeguards and enforceable data subject rights.

Effective legal remedies must also be available to data subjects.[1128] The safeguards may be provided by legally binding and enforceable instruments between public authorities or bodies,[1129] binding corporate rules,[1130] standard data protection clauses approved by the Commission,[1131] an approved code of conduct,[1132] or an approved certification mechanism.[1133]

5.9.1 Transfers of personal data based on an adequacy decision

[1124] Article 45(1) and (3) of the General Data Protection Regulation and Roos 2020 *Comparative and International Law Journal of Southern Africa* 5.
[1125] Article 45 (2) of the General Data Protection Regulation.
[1126] Article 45(2)(a) of the General Data Protection Regulation.
[1127] P Blume "EU Adequacy Decisions: The Proposed New Possibilities" (2015) 5 *IDPL* 34 and Roos 2020 *Comparative and International Law Journal of Southern Africa* 5.
[1128] Article 45(2)(a) and 46(1) of the General Data Protection Regulation.
[1129] Article 46(2)(a) of the General Data Protection Regulation, Roos 2020 *Comparative and International Law Journal of Southern Africa* 6 The Privacy Shield agreement between the EU and the USA was an example of this. The Privacy Shield replaced the Safe Harbor Agreement after its invalidation by *Maximillian Schrems v Data Protection Commissioner*, Case C- 362/14, 6 October 2015. It was adopted on 27 April 2016 and became operational on 1 August 2016. The European Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–US Privacy Shield, C (2016) 4176 final (12 July 2016). However, on 16 July 2020, the CJEU in *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* Case C-311/18 invalidated the Privacy Shield Decision because the US law assessed by the court did not provide an essentially equivalent level of protection to the EU.
[1130] Article 47 of the General Data Protection Regulation.
[1131] Article 46(2)(c) and (d) of the General Data Protection Regulation.
[1132] Article 40 and 46(2)(e) of the General Data Protection Regulation.
[1133] Article 42 and 46(2)(f) of the General Data Protection Regulation.

Article 45(2)(b) states that to process personal data to a third country using cloud computing services, there must be an existence and effective functioning of one or more independent SAs. These SAs must be established in the third country, or an international organisation is subject to. The SAs have the responsibility for ensuring and enforcing compliance with the data protection rules. These rules include adequate enforcement powers for assisting and advising the data subjects in exercising their rights and cooperation with the SAs of the Member States.[1134]

The other element is that the international commitments with the third country or international organisation concerned must be entered into.[1135] Other obligations arising from legally binding conventions or instruments and their participation in multilateral or regional systems, particularly in relation to the protection of personal data, should be considered.[1136]

After assessing the adequacy of the level of protection, the Commission may decide, by means of implementing the act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection as per the GDPR.[1137] The implementing act shall provide for a mechanism for a periodic review, at least every four years.[1138] The review shall consider all relevant developments in the third country or international organisation.[1139] The implementing act shall specify its territorial and sectoral application. Where applicable, identifying the SA referred to is also considered for the assessment.[1140] The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).[1141]

The Commission shall, following the review, that a third country, a territory or one or more specified sectors within a third country or an international organisation no longer

[1134] Article 45(2)(b) of the General Data Protection Regulation.
[1135] Article 45(2)(c) of the General Data Protection Regulation.
[1136] *Ibid*.
[1137] Article 45 (3) of the General Data Protection Regulation.
[1138] *Ibid*.
[1139] *Ibid*.
[1140] *Ibid*.
[1141] *Ibid* and Article 93 provides the provisions for the committee procedure.

ensures an adequate level of protection. The Commission will then repeal, amend or suspend its decision by means of implementing acts without retroactive effect.[1142] Those implementing acts shall be adopted in accordance with the examination procedure referred to in the GDPR.[1143]

On justified grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure as per the GDPR.[1144] The Commission shall further consult with the third country or international organisation to remedy the situation and ensure data protection adequacy.[1145] On the other hand, the POPI Act does not provide a similar provision. Although the IR is established, which performs similar functions as the SAs, the POPI Act does not explicitly clarify the role of the IR on international data flows as the GDPR does. In fact, there is no mention of the IR under section 72 of the POPI Act.

In a recent CJEU decision in *Schrems and Facebook Ireland v Data Protection Commissioner*[1146] on finding that the EU-US Privacy Shield is invalid, and its additional findings with respect to standard contractual clauses close off critical mechanisms for transferring personal data from the EU to the US, with important impacts on trade and the development of technologies such as cloud computing and AI.[1147]

In an earlier case of the CJEU decision in *Schrems v Data Protection Commissioner* [1148] found that the European Commission adequacy decisions concerning the EU-US Safe Harbor were invalid. The Commission had to revise and revoke the adequacy decision against the US-based on this decision. The importance of data flows for transatlantic economic relations necessitated that the U.S. and EU

[1142] Article 45 (5) of the General Data Protection Regulation.
[1143] *Ibid*.
[1144] *Ibid*.
[1145] Article 45 (6) of the General Data Protection Regulation.
[1146] CJEU (2020) C-311/18.
[1147] J P Meltzer "The Court of Justice of the European Union in Schrems II: The Impact of the GDPR on Data Flows and National Security" (5 August 2020) *Brookings* https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/#footnote-1 (Accessed 09 August 2020).
[1148] CJEU (2015) C-362/14.

engage in a third attempt to develop a mechanism that would enable data flows and pass muster with the CJEU.[1149]

The POPI Act does not provide a detailed list of elements as highlighted under Article 45(2) of the GDPR that should be considered when assessing the adequacy level of data protection. The Act merely states that the recipient must be subject to a law, binding corporate rules or binding agreements which provide an adequate level of protection. The Act does not mention what level such examples should be at to meet the adequacy level of data protection since the Act places such adequacy based on reasonableness which is also not articulated.

5.9.2 Transfers of personal data are subject to appropriate safeguards

A controller may transfer personal data to a third country or an international organisation only if the controller and the cloud computing service provider have appropriate safeguards.[1150] Personal data can also be transferred on the condition that enforceable data subject rights and effective legal remedies for data subjects are available in that third country.[1151]

The appropriate safeguards referred to in this context may be provided without requiring any specific authorisation from the SA.[1152] This can be achieved by a legally binding and enforceable instrument between public authorities or bodies.[1153] Binding corporate rules can also achieve it following Article 47.[1154] A standard data protection clause adopted by the Commission in accordance with the examination procedure can also be employed.[1155] A standard data protection clause adopted by a SA and approved by the Commission according to the examination procedure is also vital to

[1149] Meltzer "The Court of Justice of the European Union in Schrems II: The Impact of the GDPR on Data Flows and National Security".
[1150] Article 46 (1) of the General Data Protection Regulation.
[1151] *Ibid*.
[1152] Article 46 (2) of the General Data Protection Regulation.
[1153] Article 46 (2)(a) of the General Data Protection Regulation.
[1154] Article 46 (2)(b) of the General Data Protection Regulation and Article 47 provides binding corporate rules.
[1155] Article 46 (2)(c) and 93(2) of the General Data Protection Regulation.

ensure the proper safeguard of personal data stored in the servers of the cloud computing service provider.[1156]

An approved code of conduct[1157] together with binding and enforceable commitments of the controller in the third country to apply the appropriate safeguards, including data subjects' rights must be established.[1158] Furthermore, an approved certification mechanism[1159] together with binding and enforceable commitments of the controller in the third country must apply the appropriate safeguards, including data subjects' rights.[1160]

Subject to the authorisation from the competent SA, the appropriate safeguards referred to may also be provided.[1161] The safeguards can be achieved through contractual clauses between the controller and the controller, or the recipient[1162] of the personal data in the third country or international organisation.[1163] Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights could also suffice.[1164]

In this context, the GDPR is much more detailed on what constitute "appropriate safeguards" and the enforcement mechanisms of such agreements. The POPI Act does provide provisions for such safeguards. However, the provision is shallow as compared to the GDPR. Section 72(1) only states that the recipient must be subject to, amongst other things, a "binding agreement" which provides an adequate level of data protection. The provision does not prescribe what constitutes a binding agreement and the enforcement mechanisms to ensure adequate data protection.

5.9.3 Binding corporate rules on the transfer of personal data to third countries

[1156] Article 46 (2)(d) of the General Data Protection Regulation.
[1157] Article 40 of the General Data Protection Regulation.
[1158] Article 46 (2)(e) of the General Data Protection Regulation.
[1159] Article 42 of the General Data Protection Regulation.
[1160] Article 46 (2)(f) of the General Data Protection Regulation.
[1161] Article 46 (3) of the General Data Protection Regulation.
[1162] Article 46 (3)(a) of the General Data Protection Regulation.
[1163] *Ibid*.
[1164] Article 46 (3)(b) of the General Data Protection Regulation.

The competent SA shall approve binding corporate rules following the consistency mechanism set out in Article 63 of the GDPR.[1165] The term “binding corporate rules” means personal data protection policies adhered to by a controller or processor established on the territory of a Member State. These rules are for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings,[1166] or a group of enterprises engaged in a joint economic activity.[1167]

This is provided that the corporate rules are legally binding and apply to and are enforced by every member concerned of the group of undertakings or group of enterprises engaged in a joint economic activity, including their employees.[1168] It could also be the fact that they expressly confer enforceable rights on data subjects with regard to the processing of their data[1169] and fulfil the requirements laid down by the GDPR.[1170]

The binding corporate rules shall specify the structure and contact details of the group of undertakings or groups of enterprises engaged in joint economic activity and each of its members.[1171] It could also be the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes. The type of data subjects affected and the identification of the third country or countries in question is also considered.[1172] The corporate rules must be ensured of their legally binding nature, both internally and externally in the EU.[1173]

The binding corporate rules do not bind the general data protection principles; however, they must be included in the corporate rules.[1174] In particular, the purpose

[1165] Article 47(1) of the General Data Protection Regulation and Article 63 provides the Regulation consistency mechanism provisions.
[1166] Article 4(19) of the General Data Protection Regulation “group of undertakings” means controlling undertakings and controlled undertakings.
[1167] Article 4 (20) of the General Data Protection Regulation.
[1168] Article 47(1)(a) of the General Data Protection Regulation.
[1169] Article 47(1)(b) of the General Data Protection Regulation.
[1170] Article 47(1)(c) of the General Data Protection Regulation.
[1171] Article 47(2)(a) of the General Data Protection Regulation.
[1172] Article 47(2)(b) of the General Data Protection Regulation.
[1173] Article 47(2)(c) of the General Data Protection Regulation.
[1174] Article 47(2)(d) of the General Data Protection Regulation.

limitation, data minimisation, limited storage periods, data quality, data protection by design and default, also, the legal basis for processing, processing special categories of personal data, measures to ensure data security, and the requirements regarding onward transfers to bodies should be included.

The rights of data subjects regarding the processing and the means to exercise those rights must be specified in the corporate rules.[1175] These include the right not to be subject to decisions solely on automated processing, including profiling. The right to lodge a complaint with the competent SA and before the competent courts of the Member States must also be specified. The affected data subject must obtain redress, and, where appropriate, compensation for a breach of the binding corporate rules must be provided and specified.[1176]

The controller must establish a clear acceptance on the territory of a Member State of liability for any breaches of the binding corporate rules.[1177] The controller shall be exempt from that liability, in whole or in part, only if it proves that it is not responsible for the event giving rise to the damage.[1178]

The Commission may specify the format and procedures for exchanging information between controllers, processors and SAs for binding corporate rules within the meaning of the GDPR. Those implementing acts shall be adopted in accordance with the examination procedure set out in the GDPR.[1179] The POPI Act has a similar definition for the term “binding corporate rules” under section 72(2)(a). The GDPR, however, does not only define the term “binding corporate rules” in a passive mode like the POPI Act does. The GDPR further outlines how the binding corporate rules should be designed, their scope, application, and enforcement mechanisms. The POPI Act is undoubtedly inadequate in regulating this provision of “binding corporate rules” against the GDPR.

[1175] Article 47(2)(e) of the General Data Protection Regulation.
[1176] *Ibid*.
[1177] Article 47(2)(f) of the General Data Protection Regulation.
[1178] *Ibid*.
[1179] Article 47(3) and 93(2) of the General Data Protection Regulation.

5.9.4 Transfers or disclosures not authorised by EU law

When the controller or the cloud computing service provider has processed personal data without the necessary disclosure or authorisation, such processing is deemed unlawful.[1180] The GDPR provides that any judgement of a court or tribunal and any decision of an administrative authority of a third country requiring to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement.[1181]

These agreements include an MLA treaty in force between the requesting third country and the EU or a Member State. The MLA should be without prejudice to other grounds for transfer pursuant to chapter 5 of the GDPR.[1182] An example of one of these agreements is the EU–US Privacy Shield Agreement that replaced the Safe Harbor Agreement. [1183] In the South African context, section 40(1)(c)[1184] of the POPI Act makes provisions on mutual agreements with third countries.

5.9.5 Derogations for specific situations

The GDPR further provides that in the absence of adequacy or appropriate safeguards pursuant, including binding corporate rules, transferring personal data to a third country or an international organisation shall occur only under certain conditions.[1185] The first condition is that the data subject should explicitly consent to the proposed transfer. This is after informing the data subject of the possible risks of such transfer due to the absence of an adequacy decision and appropriate safeguards.[1186] The POPI Act's section 72(1)(b) has a similar provision that the data subject's consent

[1180] Article 48 of the General Data Protection Regulation.
[1181] *Ibid*.
[1182] *Ibid*.
[1183] C (2016) 4176.
[1184] Section 40(1)(c) of the Protection of Personal Information Act states that the Information Regulator has to consult with interested parties by—
(i) receiving and inviting representations from members of the public on any matter affecting the personal information of a data subject;
(ii) co-operating on a national and international basis with other persons and bodies concerned with the protection of personal information; and
(iii) acting as a mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by a responsible party in the interests of protecting the personal information of a data subject.
[1185] Article 49(1) of the General Data Protection Regulation.
[1186] Article 49(1)(a) of the General Data Protection Regulation.

must be obtained first before transferring personal information across the South African borders.

The second condition could be that the transfer is necessary for the performance of a contract. The contract must be between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.[1187] Section 72(1)(c) of the POPI Act has a similar provision.

The third condition is that the transfer must be necessary for the conclusion or performance of a contract concluded in the data subject's interest between the controller and another natural or legal person.[1188] Section 72(1)(d) of the POPI Act has a similar provision, but instead of including natural persons, the POPI Act simple refers to the other party as a third party. Since the POPI Act seems only to regulate the personal information processed by juristic persons and excludes natural persons, it will appear that the scope of the GDPR is broader than that of the POPI Act in this context.

The fourth condition is that the transfer should be necessary for important reasons of public interest,[1189] which is a provision that the POPI Act does not echo. The fifth condition pertains to the transfer necessary for establishing, exercising or defending legal claims.[1190] There is also a sixth condition stating that the transfer must be necessary to protect the data subject's vital interests or other persons, where the data subject is physically or legally incapable of giving consent.[1191]

According to EU or Member State law, the seventh condition is around the transfer made from a register intended to provide information to the public.[1192] Such data must be open to consultation either by the public in general or by any person who can demonstrate a legitimate interest. The consultation is only to the extent that the

[1187] Article 49(1)(b) of the General Data Protection Regulation.
[1188] Article 49(1)(c) of the General Data Protection Regulation.
[1189] Article 49(1)(d) of the General Data Protection Regulation.
[1190] Article 49(1)(e) of the General Data Protection Regulation.
[1191] Article 49(1)(f) of the General Data Protection Regulation.
[1192] *Ibid*.

conditions laid down by EU or Member State law for consultation are fulfilled in the particular case.[1193]

A transfer could not be based on a provision in Article 45 or 46, including binding corporate rules and no derogations for a specific situation. A transfer to a third country or an international organisation may occur only if the transfer is not repetitive.[1194] The transfer must concern only a limited number of data subjects or is necessary for compelling legitimate interests pursued by the controller. Such interests should not be overridden by the data subject's interests or rights and freedoms.

The controller has to conduct an assessment on all the circumstances surrounding the data transfer and, based on that assessment, provide suitable safeguards with regard to the protection of personal data.[1195] The controller shall inform the SA of the transfer. In addition to providing such information, the controller shall inform the data subject of the transfer and on the compelling legitimate interests pursued.[1196]

In the absence of an adequacy decision, EU or Member State law may expressly set limits to transferring specific categories of personal data to a third country or an international organisation. The Member States shall notify such provisions to the Commission.[1197] The controller and the cloud computing service provider shall document the assessment and the suitable safeguards that have been put in place for personal data protection.[1198]

[1193] Article 49(1)(g) of the General Data Protection Regulation.
[1194] *Ibid*.
[1195] *Ibid*.
[1196] *Ibid*.
[1197] Article 49(5) of the General Data Protection Regulation.
[1198] Article 49(6) of the General Data Protection Regulation.

5.9.6 International cooperation for the protection of personal data

Concerning third countries and international organisations, the Commission and SAs shall take appropriate steps to safeguard the personal data of EU citizens.[1199] These steps include developing international cooperation mechanisms to facilitate the effective enforcement of legislation to protect personal data.[1200]

These include notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for protecting personal data and other fundamental rights and freedoms.[1201] The Commission must engage relevant stakeholders in discussion and activities to further international cooperation in the enforcement of legislation to protect personal data.[1202] These engagements can assist in promoting the exchange and documentation of personal data protection and practices, including jurisdictional conflicts with third countries.[1203]

None compliance with the GDPR on processing personal data within and outside the EU through cross-border data processing could lead to severe consequences. The GDPR provides provisions for the remedies, liabilities and penalties for non-compliance with its provisions. It will not make sense to discuss the provisions of the GDPR in the context of cloud computing without discussing the remedial mechanisms for non-compliance with such provisions. The remedies of the GDPR will be discussed below in a cloud computing context.

5.10 Remedies and liabilities for non-compliance with the GDPR

Since the adoption of the GDPR, much attention has been centred on administrative sanctions issued by the Member State national data protection agencies for EU data protection law violations.[1204] Article 82(1) of the GDPR provides that any person who has suffered material or non-material damage due to an infringement of the GDPR shall have the right to receive compensation from the controller or the cloud computing

[1199] Article 50 of the General Data Protection Regulation.
[1200] Article 50(1)(a) of the General Data Protection Regulation.
[1201] Article 50(1)(b) of the General Data Protection Regulation.
[1202] Article 50(1)(c) of the General Data Protection Regulation.
[1203] Article 50(1)(d) of the General Data Protection Regulation.
[1204] O Tambou "Lessons from the First Post-GDPR Fines of the CNIL Against Google LLC" (2019) 5 *EUR. DATA PROT. L. REv.* 80 and O'Dell 2017 *DUBLIN U. L.J.* 49.

service provider for the damage suffered.[1205] As a consequence, compliance with the GDPR is ensured through a mutually reinforcing combination of public and private enforcement that blends public fines with private damages.[1206]

5.10.1 Right to complain with a Supervisory Authority

A natural person whose privacy has been infringed upon by processing their data can sue the controller in terms of the GDPR. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to complain with a SA.[1207] The action can be brought particularly in the Member State where the data subject is domiciled, place of work, or the alleged infringement in relation to the processing of personal data that does not comply with the GDPR.[1208]

The SA with which the complaint has been lodged shall inform the complainant of the progress and the outcome of the complaint.[1209] The progress could include aspects such as the possibility of a judicial remedy pursuant to Article 78 of the GDPR.[1210] The GDPR further provides that each data subject shall have the right to an effective judicial remedy against a legally binding decision of a SA concerning them.[1211] Each data subject shall also have the right to an effective judicial remedy where the competent SA does not handle a complaint or inform the data subject within three months on the progress or outcome of the complaint lodged.[1212]

Proceedings against a SA shall be brought before the courts of the Member State where the SA is established.[1213] Where proceedings are brought against a decision of a SA preceded by an opinion or a decision of the board in the consistency mechanism, the SA shall forward that opinion or determination to the court.[1214]

[1205] Article 82(1) of the General Data Protection Regulation and O'Dell 2017 *DUBLIN U. L.J.* abstract and 103.
[1206] O'Dell 2017 *DUBLIN U. L.J.* abstract.
[1207] Article 77(1) of the General Data Protection Regulation.
[1208] *Ibid*.
[1209] Article 77(2) of the General Data Protection Regulation.
[1210] *Ibid* and Article 78 provides the data subject's right to an effective judicial remedy against a supervisory authority.
[1211] Article 78(1) of the General Data Protection Regulation.
[1212] Article 78(2) of the General Data Protection Regulation.
[1213] Article 78(3) of the General Data Protection Regulation.
[1214] Article 78(4) of the General Data Protection Regulation.

On the other hand, the proceedings against a controller shall be brought before the courts of the Member State where the controller has an establishment.[1215] Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has their habitual residence. This approach cannot be employed if the controller is a public authority of a Member State acting to exercise its public powers.[1216] This provision provides some flexibility in a cloud computing context. The controller does not have to be physically present in the EU or Member State to process personal data. In this instance, the court where the data subject is domiciled also has jurisdiction to hear the matter.

5.10.2 Representation of data subjects and suspension of the proceedings

The scope of the GDPR is so broad and favours the data subjects extensively. The data subject shall have the right to mandate a non-profit body, organisation or association to complain on their behalf.[1217] The purpose of the organisation must be in the public interest.[1218] It must be active in protecting data subject rights and freedoms regarding processing their data, filing a complaint, applying to a court for relief against a SA, or seeking an effective remedy against a controller or processor on behalf of the data subject.[1219]

The mandated body must exercise the rights in Articles 77, 78 and 79 of the GDPR on behalf of the data subject. The mandated body also has to exercise the right to receive compensation under Article 82 on behalf of the data subject.[1220] Member States may provide that anybody, organisation or association mandated, independently of a data subject's mandate, has the right to complain with the SA in that Member State.[1221]

5.10.3 Right to compensation and liability for unlawful processing of personal data

[1215] Article 78(3) of the General Data Protection Regulation.
[1216] Article 79(2) of the General Data Protection Regulation.
[1217] Article 80 of the General Data Protection Regulation.
[1218] O'Dell 2017 *DUBLIN U. L.J.* 54.
[1219] *Ibid*.
[1220] Article 80(1) of the General Data Protection Regulation.
[1221] Article 80(2) of the General Data Protection Regulation.

The cloud computing service provider or user is liable for the damage only where it has not complied with obligations of the GDPR specifically directed to it or where it has acted outside or contrary to lawful instructions of the controller.[1222]

A controller is exempt from liability under the GDPR if it proves that it is not in any way responsible for the event giving rise to the damage.[1223] Where more than one controller is involved in the same processing, they are both responsible for any damage caused by processing personal data unlawfully.[1224] Each controller shall be held liable for the entire damage to ensure effective compensation of the data subject.[1225]

5.11 Penalties for non-compliance with the GDPR

Penalties for non-compliance with the GDPR are, on the face of it, severe. Each SA shall ensure that the imposition of administrative fines pursuant to the GDPR for its infringements shall be effective, proportionate, and dissuasive in each case.[1226] Depending on the matter, administrative fines are imposed on controllers or cloud computing service providers on a case-by-case basis.[1227] The penalties can be imposed instead of measures referred to in Article 58(2).[1228] In each case, due regard shall be given when deciding on imposing an administrative fine or the amount of the administrative penalty.

The consideration includes the nature, gravity and duration of the infringement. The tribunal must consider the nature, scope or purpose of the processing concerned, the number of data subjects affected, and the level of damage suffered by them.[1229] The two categories of provisions set out in Article 83 of the GDPR may be broken down into infringements considered less severe and considered more serious.[1230] The less serious include infringement of provisions centred around compliance ensuring

[1222] Article 82(2) of the General Data Protection Regulation.
[1223] Article 82(3) of the General Data Protection Regulation.
[1224] Article 82(4) of the General Data Protection Regulation.
[1225] *Ibid*.
[1226] Article 83(1) of the General Data Protection Regulation.
[1227] *Ibid*.
[1228] Article 83(2) of the General Data Protection Regulation.
[1229] Article 83(2)(a) of the General Data Protection Regulation.
[1230] O'Dell 2017 *DUBLIN U. L.J.* 59.

obligations, including specific security obligations.[1231] The more severe include infringement of provisions centred around essential obligations to process data and data subjects' rights.[1232]

There must be an assessment to determine if the unlawful act was an intentional or negligent character of the infringement.[1233] The POPI Act provides a similar provision. Section 99 provides for liability without fault; whether the act or omission was negligent or intentional, the provisions of the POPI Act will still apply.

Any action taken by the controller to mitigate the damage suffered by data subjects must be considered when deciding on the matter.[1234] The degree of responsibility of the controller, taking into account technical and organisational measures implemented by them, is also considered when deciding on the matter.[1235] The tribunal further determines any relevant previous infringements by the controller or cloud computing service provider.[1236]

The degree of cooperation with the SA to remedy the infringement and mitigate the possible adverse effects of the infringement is also vital to decide on the matter.[1237] The tribunal considers the categories of personal data processed through cloud computing services affected by the infringement.[1238]

How the infringement became known to the SA, particularly whether, to what extent the controller notified the data subjects about the infringement, must be considered.[1239] The tribunal will further consider the adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms in accordance

[1231] W G Voss "Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later" (2014) 17 *J. INTERNET L.* 1 at 19 to 21 and Article 83(4) of the General Data Protection Regulation.
[1232] Voss 2014 *J. INTERNET L.*19 to 21 and Article 83(5) of the General Data Protection Regulation.
[1233] Article 83(2)(b) of the General Data Protection Regulation.
[1234] Article 83(2)(c) of the General Data Protection Regulation.
[1235] Article 83(2)(d) of the General Data Protection Regulation.
[1236] Article 83(2)(e) of the General Data Protection Regulation.
[1237] Article 83(2)(f) of the General Data Protection Regulation.
[1238] Article 83(2)(g) of the General Data Protection Regulation.
[1239] Article 83(2)(h) of the General Data Protection Regulation.

with Article 42.[1240] Any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits gained or losses avoided, directly or indirectly, from the infringement is, taken into consideration.[1241]

The GDPR states that if a controller intentionally or negligently infringes several provisions of the GDPR for the same or linked processing operations, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.[1242]

The GDPR provides a list of infringements subject to administrative fines up to 10000000EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year or whichever is higher.[1243] These infringements include (a) The obligations of the controller as provided under Articles 8, 11, 25 to 39, 42 and 43 of the GDPR.[1244] (b) The obligations of the certification body as outlined under Articles 42 and 43 of the GDPR[1245] and (c)the obligations of the monitoring body pursuant to Article 41(4) of the GDPR.[1246]

The other category of infringements is subject to administrative fines up to 20000000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.[1247]
(a) The basic principles for processing, including conditions for consent, are indicated under Articles 5, 6, 7 and 9.[1248]
(b)The data subjects, rights pursuant to Articles 12 to 22 as contained in the GDPR.[1249]

[1240] Article 83(2)(j) of the General Data Protection Regulation.
[1241] Article 83(2)(k) of the General Data Protection Regulation.
[1242] Article 83(3) of the General Data Protection Regulation.
[1243] Article 83(4) of the General Data Protection Regulation, Von dem Bussche-Freiherr *European Data Protection Law Review* 581, Schildhaus 2017 *INT'l L. News* 12, Rosentau 2018 *JURIDICA INT'l* 39 and Voss 2020 *Santa CLARA HIGH TECH. L. J.* 8.
[1244] Article 83(4)(a) of the General Data Protection Regulation.
[1245] Article 83(4)(b) of the General Data Protection Regulation.
[1246] Article 83(4)(c) of the General Data Protection Regulation.
[1247] Article 83(5) of the General Data Protection Regulation, Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 581 and Voss 2020 *Santa CLARA HIGH TECH. L. J.* 8.
[1248] Article 83(5)(a) of the General Data Protection Regulation.
[1249] Article 83(5)(b) of the General Data Protection Regulation.

(c) The transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49 by the controller using cloud computing services unlawfully can lead to such a hefty fine.[1250]

(d)Any obligations pursuant to Member State law adopted under Chapter IX of the GDPR is also punishable up to 20000000 EUR, or up to 4 % of the total worldwide annual turnover of the controller.[1251]

Non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the SA pursuant to Article 58(2) can lead to a similar fine. Failure to provide access in violation of Article 58(1) also leads to a fine of 20000000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover.[1252]

Non-compliance with an order by the SA as referred to in Article 58(2) shall be subject to administrative fines up to 20000000 EUR, or up to 4% of the total worldwide annual turnover of the preceding financial year whichever is higher.[1253] Without prejudice to the corrective powers of SA under Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State in the EU.[1254]

The exercise by the SA of its powers under the GDPR shall be subject to appropriate procedural safeguards in accordance with EU and Member State law. These include effective judicial remedy and due process should an international data breach occur or unlawful processing of personal data has materialised in a cloud computing context.[1255]

[1250] Article 83(5)(c) of the General Data Protection Regulation.
[1251] Article 83(5)(d) of the General Data Protection Regulation and Voss 2020 *Santa CLARA HIGH TECH. L. J.* 8.
[1252] Article 83(5)(e) of the General Data Protection Regulation and Rosentau 2018 *JURIDICA INT'l* 39.
[1253] Article 83(6) of the General Data Protection Regulation, Schildhaus 2017 *INT'l L. News* 12 and Rosentau 2018 *JURIDICA INT'l* 39.
[1254] Article 83(7) of the General Data Protection Regulation.
[1255] Article 83(8) of the General Data Protection Regulation.

Where the Member State's legal system does not provide for administrative fines, provisions of Article 83 may be applied in such a manner that the competent SA initiates it. The penalty can also be imposed by competent national courts while ensuring that those legal remedies are effective and equivalent to the administrative fines imposed by SA.[1256] The fines imposed shall be effective, proportionate, and dissuasive in any event.[1257]

5.12 Shortcomings of the GDPR

The GDPR does not provide a complete set of rules for all relevant areas of data protection law. It has certain opening clauses allowing Member States to fill in the gaps with national law, albeit in line with the general principles of the GDPR. One prominent example is employee data protection which remains in the legislative power of the Member State as shown in Article 88. It is yet to be seen whether a supplement of all the EU Member States' national laws will facilitate the pan European application of the GDPR. More likely, a partly harmonised but still highly fragmented data protection landscape will remain.[1258]

The GDPR covers a broad scope of its jurisdictional reach across the world. These territorial provisions limit the opportunity for law-shopping and may be seen to allow a more level playing field for European companies in the face of other regions such as North America, Africa or even East Asian competitors in the borderless world of the Internet.[1259] The GDPR also does not provide data protection to juristic persons.

5.13 Conclusion

Based on the analysis above, it is clear that in most instances, data controllers or responsible parties who utilise cloud computing services to process personal information in SA and the EU stand an excellent chance to succeed in harmonising their approach to be compliant with both legislations.[1260] There are some significant

[1256] Article 83(9) of the General Data Protection Regulation.
[1257] *Ibid*.
[1258] Von dem Bussche-Freiherr 2016 *European Data Protection Law Review* 581.
[1259] Voss 2016 *R.J.T. n.s.* 800.
[1260] Yav 2018 *International Journal Data Protection Officer, Privacy Officer and Privacy Counsel* 20.

differences between these two pieces of legislation; therefore, it would be prudent to highlight those differences in detail and provide recommendations for the legislature to attend to the provisions that do not reach the standard set by the GDPR before approaching the EU for a declaration of adequacy. The following chapter will discuss the differences between the POPI Act and the GDPR. Based on the research findings, the discussion will provide recommendations before concluding the research study.

Chapter 6: Recommendations and Conclusion

6.1 Introduction

It is submitted that the goals and the research questions raised in chapter one of this study have been addressed.[1261] Each chapter addressed different aspects of the regulation of cloud computing and the right to privacy in South Africa with reference to other international legal instruments as discussed in the study.

The purpose was to respond to the research problem posed, which was to analyse and determine whether the POPI Act can offer adequate data protection in the form of remedies and enforcement mechanisms for international data breaches in cloud computing services and the protection of the right to privacy.[1262] The responses to the research problem were addressed in the study and highlighted in the findings below. Therefore, based on the analysis from the previous chapters, this last chapter of the research will summarise the research, the findings of the study, the recommendations and the conclusion of the chapter.

6.2 Summary of thesis

The study highlighted that the introduction of cloud computing has become a global concern in the IT space and the right to privacy. Regulation of data protection remains vital to ensure the strict guidelines and enforceability of data privacy in the context of cloud computing, as illustrated by the promulgation of the GDPR and the POPI Act above.

The concerns around cloud computing services are raised and shared by the legal community, who in different areas face the challenge of providing adequate protection and dealing with some other legal issues around the cloud computing model. There is also a challenge of understanding the proper law applicable to cloud computing

[1261] See the Goals of the Research as discussed in paragraph 1.4 in Chapter 1, page 9 of the research.
[1262] See the main aim under the Goals of the Research as outlined in paragraph 1.4 in Chapter 1, page 9 of the research.

technology. The analysis above has highlighted some of these challenges. The thesis highlighted the inadequacies of data protection in the cloud computing context under the common law and the Constitution. It has further highlighted some gaps within the POPI Act and the GDPR. Furthermore, these are not the only challenges identified; the uniqueness of some of these challenges may further be summarised as highlighted below.

The growing phenomenon of cloud computing services has attracted the attention of legislators and government officials across the globe. These bodies sometimes see themselves as users, regulators, controllers and sometimes researchers.[1263]

As users, governments are adopting public, private and hybrid cloud computing deployments for operational use to take advantage of its financial and technical efficiency, innovative features and ability to facilitate collaborative environments.[1264] However, the governments also play the role of regulators of cloud computing services. The governments have a fiduciary duty to formulate and implement legislation, judicial and regulatory agencies and bodies to protect the personal information of its citizens while implementing guidelines for the cloud computing service providers and the users.

As researchers, governments are further faced with a challenge to understand the technical problems and information society challenges that technology presents in research initiatives conducted directly by the government or by private organisations it funds.[1265] As controllers or responsible parties, the governments also utilise cloud computing platforms to process personal information for certain activities such as census, voter's roll, birth certificates, death certificates, marriage registrations, and tax collection.

The study has further indicated that the POPI Act provides provisions and conditions for the lawful processing of personal information. The POPI Act's provisions provide

[1263] Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 247.
[1264] *Ibid*.
[1265] Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 247 to 248.

"adequate" data protection standards to secure SA's participation in the international trade market.[1266] Because cloud computing involves massive cross-border data flows, the POPI Act provides provision for personal information across SA borders, which the constitutional and the common law mechanisms fall short of.

The major challenge of the POPI Act is that the GDPR has more binding force and is much updated with the growth of technology than its predecessor, the Directives, which the POPI Act was built upon. The arising concern is whether the POPI Act still meets the minimum standard of data protection set out by the GDPR or whether the revision of specific provisions of the POPI Act is needed.

Chapter 5 of the study provided a comparative analysis of the GDPR and the POPI Act with regard to the content of specific concepts and the legal bases for lawful processing of personal information both in the EU and SA. The analysis highlighted that certain concepts for the POPI Act and the GDPR are equivalent. Based on the analysis for lawful processing of personal information, there are indeed differences in data protection regulation between the two legislations. Since the GDPR has set the benchmark for an international data protection standard, the recommendations below will suggest how the POPI Act should be amended to comply with the standard set in the GDPR.

Roos has indicated that one could argue that these differences are not substantial enough to derail an adequate finding by the European Commission.[1267] However, Roos further states that it would be prudent for the legislature to bolster the provisions that do not reach the standard set by the GDPR before approaching the EU for such a declaration.[1268] Based on the analysis from the previous chapters of the study, specific findings have been identified. These findings, as highlighted below, will assist in composing and providing some recommendations on how the data protection laws in SA, especially the POPI Act, can be developed and redefined to meet the

[1266] Neethling *et al Neethling on Personality Rights* 414 and Naude and Papadopoulos (2) 2016 *THRHR* 229.
[1267] Roos 2020 *Comparative and International Law Journal of Southern Africa* 31.
[1268] *Ibid*.

international data protection standards. The findings of the study are provided and analysed in the following section.

6.3 Findings

There are significant benefits and opportunities associated with the cloud computing model. However, there is still a substantial lack of understanding of the benefits and their inner workings despite this. Firstly, cloud computing users lose exclusive control over the personal data they upload on cloud computing platforms because the information is being processed and stored on servers located elsewhere in the world. The study revealed that most cloud computing users, especially ordinary people, have little knowledge of cloud computing platforms' technical and security details. This entails a lack of education to the public, cloud computing users and the data subject as far as cloud computing services are concerned.

If the cloud computing service client is not in control of the data, they may also not know all the possible security risks that their information is subject to. Computers are also vulnerable to threats such as data breaches and hacking. These risks make it imperative that both public and private bodies safeguard the personal information they process by, for example, implementing strong firewalls, policies, and procedures and regulating the industry properly.

6.3.1 Jurisdictional scope and the applicability of the POPI Act

Chapter two of the study discussed the jurisdictional issues of cloud computing. The research highlighted the jurisdictional issues surrounding the regulation of cloud computing and its impact on the right to privacy. The transnational characteristic of cloud computing function makes jurisdictional issues a critical concern to be addressed. The cross-border flow of personal information through multiple jurisdictions poses a challenge for the regulators. The significant problems of jurisdiction on cloud computing are determining how and where infringements may be resolved, which law is applicable and which courts or bodies have the authority to hear and resolve the matter.

However, with territorial location, cross-border data flows, and jurisdictional complexities, the discussion opened up in particular to the virtual operational characteristics of cloud computing.[1269] The discussion determined whether the regulators have considered all the changing aspects of cloud computing when developing policies and regulations.[1270] An excellent example in this context is the EU–US Safe Harbour Agreement which was aimed at assisting in providing cross-border data flows protection between the EU Member States and the US.

After the Safe Harbour agreement was declared invalid, the EU and the US further enacted the new Privacy Shield Framework Regulation, upgrading the Safe Harbour protection laws. The Privacy Shield provide extended forms of data transmission and cross-border data protection between the EU and the US, while SA also provide the limitation of liability protection through section 72 of the POPI Act.

The discussion, however, provided a high-level view of the legal status and principles that support allowing the use of cloud computing legitimately. These principles also offer enforcement measures to international data breaches, such as subjective and objective territorial principles.

The governments and the private sector are on a quest to adopt “borders” through a legal framework with extraterritorial reach on cloud computing to comply with the territorially defined regulations. While it is possible to have sector-specific regulations through regional or geolocation tools, this method of choice will not be the territorial practice of internet or cloud computing restrictions in the future.[1271] However, authorities are attempting to look for network neutrality solutions and unified global distribution to resolve these issues.[1272] This is also evidenced by extraterritorial jurisdiction components on data protection laws such as Article 44 of the GDPR and section 72 of the POPI Act.

[1269] Jackson *Legal Concerns Arising from the Use of Cloud Technologies* 248.
[1270] *Ibid*.
[1271] *Ibid*.
[1272] *Ibid*.

After analysing the provisions of both the POPI Act and the GDPR, the research indicated that many of the foundational principles of data protection and privacy are common to both laws; however, there are some variations in implementation. Firstly, the GDPR sets a minimum standard for all members of the EU, while POPI Act is limited to South Africa. Secondly, while POPI Act applies only to personal information processed within the borders of South Africa, the GDPR applies to the personal data of all EU data subjects, regardless of where such personal information is processed, that is territorial jurisdiction. Thirdly, the POPI Act encompasses the personal information of legal entities and not just individuals, making POPI Act more extensive and stringent than the GDPR in this area.

6.3.2 Issue of data subject consent

The GDPR defines consent as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by explicit affirmative action, signifies agreement to the processing of personal data relating to them.[1273] The POPI Act also describes consent in more detail, although not as detailed as the GDPR. It defines "consent" as any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.[1274] The POPI Act does not stipulate what information the data subject must be made aware of for the consent to be considered to be informed, at a minimum.

The POPI Act places the burden of proof that the data subject has consented to the responsible party.[1275] It also provides that consent may be withdrawn at any time. Such withdrawal will not affect the lawfulness of the processing of personal information before such withdrawal.[1276] In the POPI Act, the age of consent is 18 years. In the case of a child under the age of 18, the person who is legally competent to consent to any action or decision being taken regarding any matter concerning the child (referred

[1273] Article 4(11) of the General Data Protection Regulation.
[1274] Section 1 of the Protection of Personal Information Act.
[1275] Section 11(2)(a) of the Protection of Personal Information Act and Roos 2020 *Comparative and International Law Journal of Southern Africa* 17.
[1276] Section 11(2)(b) of the Protection of Personal Information Act and Roos 2020 *Comparative and International Law Journal of Southern Africa* 17.

to as the “competent person”) must consent on behalf of the child.[1277] Under the GDPR, the age of consent is 16 years, of which the POPI Act provide a better age restriction than the GDPR.

Considering the specific grounds on which processing is allowed, certain differences become apparent. The POPI Act and the GDPR list six grounds for the lawful processing of personal information that is not considered special personal information; these grounds are similar. However, on closer inspection, a few subtle differences influence the level of protection provided to data subjects in certain circumstances. Consent is a valid ground for processing in both legislative instruments. However, the GDPR spells out the requirements for valid consent in more detail, and these requirements are arguably at a higher level than those of the POPI Act.

6.3.3 Roles and definitions

The other finding was that the POPI Act confines the pivotal roles which an organisation as a user of cloud computing services may take when handling data to personal information controllers and personal information processors. On the other hand, the GDPR extends its scope and recognises additional roles such as jointly responsible parties, third parties, and recipients. However, the POPI Act defines the terms; it does not provide a broader scope than the GDPR.

6.3.4 Data protection officers

Both legislations require the appointment of an officer responsible for overseeing data protection strategy and implementation to ensure compliance with the relevant data protection provisions. The GDPR requires the appointment of a DPO for some organisations.[1278] This provision immediately excludes certain organisations from the application of the GDPR. The POPI Act has a similar provision; however, the definition is slightly different.[1279] The term “Information Officer” is used under the POPI Act.[1280]

[1277] Section 1 and 11(1)(a) of the Protection of Personal Information Act and Roos 2020 *Comparative and International Law Journal of Southern Africa* 17.
[1278] Article 37 of the General Data Protection Regulation.
[1279] Sections 55 of the Protection of Personal Information Act.
[1280] Section 1 of the Protection of Personal Information Act and Yav 2018 *International Journal Data Protection Officer, Privacy Officer and Privacy Counsel* 19.

The differentiating factor is that the POPI Act requires all organisations to have an Information Officer, in the absence of an appointed one, the responsibility falls to the head of the organisation.[1281]

6.3.5 Privacy by design and the impact assessment provisions

Privacy by design calls for privacy to be considered throughout a whole value chain process for the lawful processing of personal information benchmarks using cloud computing platforms. This will include building privacy into the design, operation, and management of a given system, business process, or design specification on all responsible parties using cloud computing services to process personal information. While the GDPR mandates the concept of privacy by design,[1282] the POPI Act does not impose an obligation on organisations that use cloud computing services.[1283] Under the POPI Act, the concept is voluntary, which opens up a leeway for organisations to accept or not accept this provision.[1284] In addition to that mandate under the GDPR is the obligation to conduct data protection impact assessments and maintain records of such assessments; this is another aspect that the POPI Act does not specify.[1285]

6.3.6 Data portability

Data protection laws are enacted to regulate how organisations should conduct themselves when processing personal information using cloud computing services. They are also enacted to provide data subjects with rights to determine how their personal information should be processed and the remedial mechanisms when those rights are breached. The concept of data portability is one of the most important concepts echoed in the GDPR in terms of warranting control rights to the data subjects.[1286] The data subjects in the EU enjoy the benefits of data portability, meaning that they can order data controllers using cloud computing platforms that their data is

[1281] Section 56 of the Protection of Personal Information Act.
[1282] Article 25 of the General Data Protection Regulation.
[1283] Yav 2018 *International Journal Data Protection Officer, Privacy Officer and Privacy Counsel* 20.
[1284] *Ibid* and section 2(1)(d) of the Protection of Personal Information Act.
[1285] Yav 2018 *International Journal Data Protection Officer, Privacy Officer and Privacy Counsel* 20.
[1286] *Ibid* and Article 20 of the General Data Protection Regulation.

transferred from one controller or service provider to another. This is a concept that is not addressed in the POPI Act.

6.3.7 Notification requirements and the penalties

The main difference between the POPI Act and the GDPR in terms of notification requirements and penalties are in regard to more stringent time constraints and more severe fines imposed by the GDPR. The GDPR places a duty on any breached organisation or cloud computing service provider to report to SA within 72 hours of discovering a breach.[1287] On the other hand, the POPI Act is vague as it does not provide a specific timeline, perhaps more worryingly for the affected organisations and cloud computing service providers. The fines in the GDPR for breach are significantly high. The penalties could range from 20 million Euros compared to POPI Act's R10 million fine. The GDPR also allows for penalties to be calculated as a percentage of the global annual revenue of companies (whichever of the two amounts is larger). Significantly, POPI Act also provides for criminal sanctions and fines, which the GDPR does not.

There are, of course, other provisions relating to the data protection principles, data subject rights, restrictions on onward transfer and the procedural and enforcement mechanisms, which should also be evaluated before a definitive answer can be given to the question of whether the POPI Act meets the benchmark set by the GDPR. Some of these inadequacies have already been addressed in chapters 4 and 5 of the study.

6.4 Recommendations

Though the threat might not rise to the level of a vital security interest in the form of terrorism, the individuals who utilize cloud computing services could reasonably argue that data security is of vital economic interest to the nation. Consequently, South Africa has to deem it necessary to extend extraterritorial jurisdiction in its data protection legal framework even without an identified specific harm or potential data breach.

[1287] Article 33 of the General Data Protection Regulation.

The overview of data privacy policies and regulations in South Africa indicates that its current state is well developed, however, there are prospects for continued growth to keep up with the international data protection standards. From the discussion above, the SA data protection laws can only benefit from conceptual clarity on the *de facto* nature of privacy and the international data protection standards and the consequential distinction between the personality interest such as the right to privacy.

6.4.1 Expansion of the territorial jurisdictional scope of the POPI Act

The POPI Act must expand and clarify its territorial jurisdiction as the GDPR does. The major challenge of cloud computing is its cross-border flow of personal information characteristics which requires international solid data protection laws. Therefore, it is recommended that the POPI Act consider adopting the provisions of the GDPR in this context.

Another major differentiating factor is that the POPI Act encompasses the personal information of legal entities and not just individuals, making POPI Act more extensive and stringent than the GDPR in this area. This concept must remain unchanged as it places POPI Act in a higher segment and favourable position than the GDPR on international data protection standards.

6.4.2 Development of the common law

The courts have a duty in terms of the Constitution to develop the common law. Chapter 3 of the study discussed in *Carmichele v Minister of Safety and Security*.[1288] The obligation of courts to develop the common law, in the context of section 39(2)[1289] objectives are not purely discretionary.[1290] The technology is undoubtedly outpacing the common law remedies; however, there is a need for the courts to keep on applying the relevant common law concepts in support of the legislative framework as well.

[1288] 2001 (4) SA 938 (CC) para 39.

[1289] Section 39 (2) Interpretation of Bill of Rights: - When interpreting any legislation, and when developing the common law or customary law, every court, tribunal or forum must promote the spirit, purport and objects of the Bill of Rights.

[1290] Neethling *et al Neethling on Personality Rights* 371.

The development of the common law in the context of cloud computing must be done on a case-by-case basis. Furthermore, the development of the common law on technology-based cases will also assist in closing the gap where the legislation fails to cover certain areas of the law.

Since it is unlikely that states, globally, will come together to create a cyber-treaty that specifically focuses on data protection in the context of cloud computing, customary international law developed through state practise will be the primary method for the formation of adequate data protection laws, especially with the influx of cross-border flow of personal information on cloud computing platforms.[1291]

6.4.3 Issues of data subject's consent

Consent is one of the cornerstones for the lawful processing of personal information. The GDPR and the POPI Act list data subject's consent as an important requirement for processing personal information lawfully. Based on the analysis provided above, the following is recommended. In the case of consent as a ground for processing personal information in general, it should be required that the data subject gives consent by means of clear affirmative action. [1292] This means that the data subject must have taken deliberate action signifying their consent to processing their personal information.[1293]

Roos also recommends further that in the case of consent as a ground for processing special categories of personal information, it should be required that the data subject explicitly gives such consent. [1294] In this case, Roos is of the opinion that assumed consent or implied consent should not be considered. This, however, makes sense as some responsible parties obtain consent once from the data subject and fail to disclose that their personal information will further be processed to other subordinates of the

[1291] H Lobel "Cyber War Inc.: The law of war implications of the private sectors role in cyber conflict" (2012) 47 *Texas International Law Journal* 617 at 638 and S G Bradbury "Keynote Address: Law, Privacy, and Warfare in a Digital World" (2011) *Harvard National Security Journal Symposium: Cybersecurity* http://harvardnsj.com/ (Accessed 27 June 2020).
[1292] Roos 2020 *Comparative and International Law Journal of Southern Africa* 31.
[1293] Article 29 Data Protection Working Party 14 to 15 and Roos 2020 *Comparative and International Law Journal of Southern Africa* 15.
[1294] Roos 2020 *Comparative and International Law Journal of Southern Africa* 31.

business or third parties. Therefore, the responsible parties assume consent to the processing or further processing such personal information.

In the case of processing that complies with an obligation imposed by law on the responsible party or processing that protects a legitimate interest of the data subject, it should be required that the processing is necessary to fulfil those purposes.[1295] This is another recommendation made by Roos. Roos further states that in the case of processing personal information to protect the interests of the data subject, it should be required that the interests that are to be protected are vital. It must be provided that public authorities may not use this ground as a basis for processing personal information but must instead have another legal basis provided by the legislator. [1296]

[1295] *Ibid*.
[1296] *Ibid*.

6.4.4 Roles and definitions

Both the POPI Act and the GDPR define the terms “data controller” and “responsible party” and a “processor” and the “operator”, respectively, as discussed above. However, the POPI Act refers to third parties and recipients, these two terms are not explicitly defined under the POPI Act, but they are clearly defined under the GDPR. In the context of the POPI Act, a third party appears to be someone to whom the personal information is supplied (in other words, very similar to a recipient).[1297] For example, in the section that concerns the transfer of personal information outside the Republic, the Act refers to “the third party who is the recipient of the information”.

Based on the above, it is recommended that certain terms of the POPI Act must be clearly defined as the GDPR does. This will eliminate the need to try and match certain words used on both legislations, especially in a context where the GDPR explicitly defines the terms used in the GDPR. However, despite the confusion, the meaning of these terms on both legislations is fairly similar.

6.4.5 Data protection officers

The POPI Act requires all organisations to have an Information Officer, and in the absence of an appointed one, the responsibility falls to the head of the organisation. On the other hand, the GDPR only prescribes certain organisations to have a DPO. In this context, the POPI Act undoubtedly provides a broader scope of data protection mechanism than the GDPR; therefore, this is a concept that should be kept and maintained to improve the chances of an adequate declaration of the POPI Act.

6.4.6 Privacy by design concept

The legislator must view privacy by design as one of the vital components for data protection. Organisations must be obliged to have these internal data protection measures in place to expand the POPI Act and its provisions.

These will undoubtedly help close the gaps in the POPI Act and simplify control measures and provide simplified red flags to the data processors. Besides, the GDPR

[1297] Roos 2020 *Comparative and International Law Journal of Southern Africa* 11.

that has set the benchmark for an international data protection standard makes privacy by design mandatory for all organisations. For the POPI Act to meet the required standard for a declaration of adequacy, it must comply with the requirements of the GDPR. Furthermore, making privacy by design a voluntary measure will open a gap within the organisation, and no penalties can be enforced against the failure of voluntary measures. Making privacy by design mandatory will strengthen the IR's quest to monitor and enforce the provisions and objectives of the POPI Act.

6.4.7 Data portability

It is recommended that the legislator revisit and revise the concept of data portability under certain provisions of the POPI Act, especially section 5, which outlines the data subject's rights. This is a concept that is not addressed in the POPI Act. The data subjects in the EU enjoy the benefits of data portability. Since this is one of the vital concepts in the GDPR for lawful processing of personal information and a benchmark for international data protection standards, the legislator must consider enforcing a similar provision in the POPI Act.

6.4.8 Notification requirements and penalties

Concerning the analysis provided for section 77 of the POPI Act in cloud computing under chapter 4, timelines posed a challenge for the data subjects. The POPI Act fails to provide specific timelines on different provisions, such as the notification period. The POPI Act must specify the timelines; however, keep the penalties reasonable. Having specific and clearly defined timelines help to hold the responsible parties accountable.

6.4.9 Multi-Faceted approach

A multi-faceted approach has been recommended by the International Telecommunication Union (ITU) and the OECD, and it is also part of Australia's strategy in dealing with online activities.[1298] Should South Africa take this route, this approach on cloud computing related matters will not only be in line with other

[1298] S E Mokowadi-Tladi *The Regulation of Unsolicited Electronic Communication(Spam) in South Africa: A Comparative Study* (LLD Thesis, UNISA, 2017) 303.

jurisdictions but will also be a solution that has been called for by other commentators in the world.[1299] The multi-faceted approach will therefore include the following: strong legislation, general public education on cloud computing; technical measures; industry partnerships; and international cooperation.

6.4.9.1 Adoption of assertive cloud computing specific legislation

As a critical mechanism to regulate cloud computing, SA is strongly recommended to enact a specific cloud computing legislation at the national level. The legislation should include all relevant terms for clarity, cloud computing technology-specific, and ease of reference. The legislation and terminology should also allow future cloud computing technological developments. However, it should be noted that technology keeps evolving and progressing at a tremendous speed. It is worth noting that post the adoption of certain rules and regulations, cloud computing appears to be a hindrance by the increased complexity of its operating model and environment through the introduction of new trends and technologies.

While the legal issues of some rules and regulations can be resolved through minor incremental updates, others require a more fundamental revision of the laws that provide data protection mechanisms such as the POPI Act and the Cybercrimes Act. The national and international legal framework must be prepared for the evolving cloud computing environment, and single global information cyberspace and digital legal framework is further recommended with the specific focus on cloud computing technologies.

It is important to note that in April 2021 South Africa issued a Draft National Policy on Data and Cloud.[1300] The policy seeks to create an enabling environment for data and cloud services to ensure socio-economic development for inclusivity.[1301] The objectives of this policy are to: Promote connectivity and access to data and cloud

[1299] *Ibid*.
[1300] Invitation to submit written submissions on the proposed National Data and Clod Policy: Government gazette Number 309 (44411) (1 April 2021) http//:www.gpwonline.co.za 3 (Accessed 14 May 2021).
[1301] *Ibid*.

computing services, remove regulatory barriers and enable competition.[1302] Arguably so, the recommendation made above is on the aspects of adopting primary legislation that will deal directly and provide provisions for cloud computing, seeing that various organisations are quickly adopting cloud computing services. The Notice was also issued under the Electonic Communications Act 36 of 2005, not specifically the POPI Act under discussion.

6.4.9.2 Adoption of a global cloud computing treaty and industry-specific policies

a. At national level

It is recommended that the government adopts national policies binding on all the organisations, including organisations outside the Republic that conduct their businesses in SA or process personal information of the data subjects domiciled in SA. The rules or policies on cloud computing services should be as extensive as possible and, most importantly, consider protecting data subjects. It is further recommended that the following rules should therefore be included in the cloud computing policies:

Prohibition of using cloud computing services for unlicensed organisations. The model law should prohibit the use of cloud computing platforms for all unlicensed organisations and make sure proper disclosures are made to all the targeted data subjects of the business. The provision should read as follows:

> "An organisation must not utilise cloud computing platforms, or process any personal information, for purposes such as marketing goods or services or for credit purposes unless consent has been given before such processing and the organisation in question has been licensed to make use of cloud computing platforms to process personal information".

In addition to this, only reputable and listed or gazetted cloud computing service providers must be utilised to process personal information. It is recommended that the

[1302] *Ibid*.

IR compile, update, and publish the list of all licensed organisations that use cloud computing services. The list of all reputable national and international cloud computing service providers must be made available on different platforms such as websites. The IR must have a specific monitoring and auditing mechanism on various organisations that use cloud computing platforms.

b. At international level

Because of the transnational cross-border data flow characteristic of cloud computing services, it is recommended that all the nations come together to formulate and sign a multilateral treaty on cloud computing, and SA must be part of the signatories to that international cyber treaty. Most data breaches recorded in SA originate from beyond its borders, and the laws are ill-equipped to prosecute those perpetrators. There are few cyber-attacks so far that have been reported in SA[1303] of which no prosecution has been reported on those attacks or a case law available under the POPI Act. However, the IR has made some media statement on certain recent attacks.[1304] Moreover, the POPI Act does address cross-border issues, it offers a starting point for dealing with these matters. Section 40 (1)(e) and (g) of the POPI Act mandates the IR to conduct research into this aspect and liaise with other Regulators on the application of the POPI Act.

Based on the analysis provided under chapters 4 and 5 of this study, though there are identified and indefinable gaps on the POPI Act against the GDPR that set the benchmark for an international data protection standard, the POPI Act provides adequate data protection standards. From the provisions of the POPI Act, SA should be in a position to conclude mutual agreements with other countries such as the EU

[1303] T Shapshak "Note to Transnet: Cyberattacks Only Work When there are Vulnerabilities to Exploit" (4 August 2021) *Daily Maverik* https://www.dailymaverick.co.za/opinionista/2021-08-04-transnet-ports-closed-and-were-in-the-dark/ (Accessed 28 September 2021) and J Orr "City of Johannesburg Announces Second Ransomware Attack in Recent Months" (24 October 2019) *Cyber Security Hub* https://www.cshub.com/attacks/articles/city-of-johannesburg-announces-second-ransomware-attack-in-recent-months (Accessed 28 September 2021).

[1304] Information Regulator (IR) South Africa "Information Regulator's IT Systems Affected by a Ransomware Attack on the Department of Justice & Constitutional Development" (13 September 2021) *Media Statement* https://www.justice.gov.za/inforeg/docs/ms/ms-20210913-ITsystems.pdf (Accessed 24 February 2022) and C Dolley "Cyberattacks: South Africa, You've Been Hacked" (6 November 2021) *Daily Maverick* https://www.dailymaverick.co.za/article/2021-11-06-cyberattacks-south-africa-youve-been-hacked/ (Accessed 24 February 2022).

Members States and the US on the international regulation of cloud computing services.

These should include the top countries from which the most cloud computing service providers are domiciled. This will result in partnerships that would assist SA and those countries in dealing with data flow beyond their respective borders, holding one another accountable. These agreements should be extended to community blocs such as the Southern African Development Community (SADC) and the African Union (AU), to which SA is a member and other organisations interested in eliminating the risks of data breaches through cloud computing platforms. Having the measures indicated above would place SA in a better position to bring responsible parties who process personal information unlawfully to book.

6.4.10 Enforcement mechanisms and penalties

Regarding enforcement mechanisms and penalties, it is recommended that data subjects be provided user-friendly methodologies to report unlawful processing of their personal information. These can include a website where data subjects can complain by detailing the incidents and leaving the names of those responsible parties who have unlawfully processed their personal information. The website must also allow the data subjects to log complaints anonymously to avoid being targeted, victimised or harmed by the responsible party in question.

6.4.11 Data subjects' education and awareness

Cloud computing users and data subjects' education should prioritise ensuring the lawful processing of personal information using cloud computing platforms. An informed data subject or cloud computing user will act responsibly when engaging with technology and ensure that they leave minimal or no trail of personal information that might be exploited or used unlawfully in the future.

Data subjects' education and awareness are vital to ensure that they are aware of their rights and activate them. All stakeholders should undertake this type of education. Here, the IR must play its part to carry out these educational campaigns as recommended by section 40(1)(a) of the POPI Act.

6.4.11.1 The role of responsible parties in educating the data subjects

a. The government

The role of the government, which in most cases becomes a responsible party, is vital in this process. It is recommended and instrumental in the type of education offered at learning institutions to include a syllabus on cloud computing technologies. Although there is currently learning activities offered on IT at certain grades in schools, that is only provided from grade 10 to 12 and not at all grades.[1305] Because IT lessons are only offered in the last years of grade in schools, that means only a few learners will be exposed to such education, besides, even the content of that subject is limited to specific IT issues and does not necessarily focus on cloud computing technology.

Considering that learners fall under the category of individuals who have access to smartphones, tablets, and desktop computers from an early age, they are now the majority of online platforms users, such as social media networks, which also use cloud computing platforms. By the time they engage with IT issues, they would have long been exposed to the risk of cloud computing platforms that have been highlighted above.

It is recommended that the government introduce diverse IT subjects in lower grades in schools. This can form part of the existing subjects such as consumer studies, IT studies and even life orientation.[1306] At lower grades, the content can start with introducing the basic functions of the devices that learners are already exposed to and how cloud computing can positively and negatively impact their right to privacy. This will then move on to the workings of the Internet, specifically cloud computing services and their activities in that environment, together with how their personal information can be compromised if they are not technologically savvy.[1307] The laws applicable in this area should also be known to the learners and cloud computing users or data

[1305] Mokowadi-Tladi *The Regulation of Unsolicited Electronic Communication(Spam) in South Africa* 310.
[1306] *Ibid*.
[1307] *Ibid*.

subjects. This will set the learners in the right direction towards being informed data subjects regarding cloud computing services.[1308]

The IR should further ensure that the general public is exposed to this form of education through different platforms. These could include media platforms such as radio, TV, information brochures, and even billboard advertisements. Because SA is built on democracy, for the benefit of all the SA society members, it is recommended that this kind of education be offered in all eleven official languages. This approach will ensure that all data subjects are exposed to the language they understand.[1309]

Government departments and organisations that deal with the processing of personal information must be well informed on how they should approach and make disclosures to the data subjects they process their personal information. This education should also instruct employees on the dangers of unlawful processing or sharing lists of personal information with third parties without following proper procedures. Such misconducts could lead to heavy fines, reputational damage and imprisonment.

b. Cloud computing service providers

The cloud computing service providers' role is critical in that they are providing the data storage servers and data processing platforms and in a place to inform users with information that can assist in safeguarding their activities while using cloud computing platforms.[1310] The cloud computing service providers have to notify their platform users to be technologically savvy and not disclose personal information to third parties without following the country or industry's regulations and implementing technical solid security measures such as data encryption methods and firewalls.[1311]

This can be achieved through website popup screens, newsletters on new technologies or cloud computing platforms updates and upgrades, filters, basic

[1308] *Ibid*.
[1309] *Ibid*.
[1310] *Ibid.*
[1311] *Ibid*.

security measures, and other technology tools that the cloud computing user can access to limit the risks of data breaches.

To safeguard the right to privacy, cloud computing users should be compelled to adhere to the rules and regulations set out for the lawful processing of personal information. While these measures are sound, they will be of little value if data subjects remain ignorant on how to navigate the cloud computing platforms and the laws to guide them on the lawful processing of personal information. Education will allow cloud computing users to make informed choices before using cloud computing platforms.

It is essential to note that while SA has laws in place, it is recommended that the country align its laws to protect its citizens by implementing laws and regulations that would deal with the use of cloud computing services at the national level. Once protection is in place nationally and stakeholders play their part in protecting the right to privacy while using cloud computing platforms, the next step will be to enter into mutual agreements with other countries. These agreements should also include organisations to combat cross-border data flow characteristics of cloud computing at the international level.

By following this trend, SA would have aligned itself with international best practices that they strive to achieve in their data protection oriented laws. While there is no guarantee that these measures will eradicate all the risks associated with cloud computing and data breaches, as has been noted in other jurisdictions such as the EU, at least with such an alignment, responsible parties will be compelled to adjust their behaviour to comply with the measures put in place. On the other hand, data subjects would have received vital, albeit elusive, education to assist them in knowing how to navigate the cloud computing platforms they find themselves in. As such, they will be informed users and data subjects who will no longer be victims or easy targets of cloud computing data breaches and other risks associated with cloud computing platforms.[1312]

[1312] *Ibid* and Techdirt 'Stop saying 'if you're not paying, you're the product'' https://www.techdirt.com/articles/20121219/18272921446/stop-saying-if-youre-not-paying-youre-products.shtml (Accessed 25 February 2022).

6.5 Conclusion

The use of cloud computing as a medium of processing personal information and its effects on the right to privacy has been emphasised throughout this thesis. SA has attempted to accommodate these to some extent. Though the POPI Act targets the core principles of data protection, it is not fully compliant with the benchmark of an international data protection standard set by the GDPR. The POPI Act further falls short of adequately regulating and addressing issues directly related to the use of cloud computing services as a mechanism to process personal information concerning the right to privacy. These shortcomings have been highlighted above, and recommendations have been provided to improve the POPI Act.

Bibliography

Legislation

Children's Act 38 of 2005.

Clarifying Lawful Overseas Use of Data Act HR.4943 of 2018.

Cybercrimes Act 19 of 2020

Dutch Personal Data Protection Act 92 of 2000.

Electronic Communications Act 36 of 2005

Electronic Communications and Transactions Act 25 of 2002.

EU–US Privacy Shield, C 4176 of 2016.

EU-US Safe Harbor Agreement C (2016) 4176.

French Criminal Penal Code of 2005.

General Data Protection Regulation 2016/679 of 2018.

German Criminal Code of 1998.

National Credit Act 34 of 2005.

Protection of Personal Information Act 4 of 2013.

Restatement (Third) of USA Foreign Relations Law of 1986.

State Liability Act 20 of 1957.

The Constitution of the Republic of South Africa, 1996.

The Foreign Intelligence Surveillance Act of 1978.

The Interpretation Act 33 of 1957.

The Promotion of Access to Information Act 2 of 2000.

The US Stored Communications Act of 1986.

The USA Patriot Act 2006.

USA Title 18 of Crimes and Criminal Procedure Act of 1948.

Reports, Regulations and Rules of Court

Council of Europe Article 29 *Data Protection Working Party* 01037/12/EN WP 196.

Information Regulator of South Africa Guidance Note on the Processing of Personal Information in the Management and Containment of Covid-19 Pandemic in terms of the Protection of Personal Information Act 4 of 2013 (POPI Act): Privacy Guidance 2.2.2. (3 April 2020).

National Data and Cloud Policy, 309, *Government Gazette Number* 44411, 1 April 2021.
Protection of Personal Information Act Proclaimation, GN R1383, *Government Gazette* 42110, 14 December 2020.
Protection of Personal Information Act Proclaimation, GN R21, *Government Gazette* 43461, 22 June 2020.
Protection of Personal Information Act Regulations, GN R25, *Government Gazette* 37544, 11 April 2014.
South African Law Reform Commission Project 124: *Privacy and Data Protection* Discussion Paper 109.
United Nations Human Rights Council Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression Supp No 3 UN Doc A/HRC/23/40 (2013) UNHRC 23rd Session.
United Nations Human Rights Council Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism UN Doc A/HRC/6/17 (2007) UNHRC 13th Session.

International treaties and agreements

Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, (28 January 2003) ETS No. 189: Strasbourg.
African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) EX.CL/846(XXV) 2014,
Arab Convention on Combating Information Technology Offences (21 December 2001) Cairo.
Charter of Fundamental Rights of the European Union 2012/C 326/02.
Communication from the European Commission to the Council and the European Parliament Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, COM (2012) 0140 final Brussels.
Computer Crime and Cybercrime, Southern African Development Community (SADC) Model Law 2013,
Convention of 1936 for the Suppression of the Illicit Traffic in Dangerous Drugs: League of Nations Treaty Number 4648 Geneva.
Council of Europe Convention on Cybercrime 23 November 2001 ETS No. 185 Budapest.

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2001 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography and Replacing Council Framework Decision 2004/68/JHA.
Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA.
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (1995) OJ L281/31.
Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–US Privacy Shield (2016) C 4176.
European Convention on Human Rights 4.XI.1950, Rome
General Agreement on Trade in Services, Marrakesh Agreement Establishing the World Trade Organization (GATS) (1994) 1869 UN Treaty Ser 183.
International Convention for the Suppression of Counterfeiting Currency (1929) League of Nations Treaty Number 2623 Geneva.
International Covenant on Civil and Political Rights (1966) United Nations Treaty Number 14668.
Organisation for Economic Co-operation Development Guidelines Governing the Protection of Privacy and Trans border Flows of Personal Data (23 September 1981) Paris.
The Charter of Fundamental Rights of the European Union Number 2000/c 364/1 of 2000.
The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention: Treaty Number 108 (28 January 1981) Strasbourg.
The European Commission, Commission Implementing Decision (EU) 2016/1250.

Case Law

Barkhuizen v Napier 2007 (5) SA 323 (CC).
Bato Star (Pty) Ltd v Minister of Environment Affairs and Tourism 2004 (4) SA 490 (CC).
Bernstein v Bester 1996 (2) SA 751 (CC).
Black v Joffe 2007 (3) SA 171 (C).

Bodil Lindqvist v Åklagarkammaren i Jönköping (2003) C-101/01.

Carmichele v Minister of Safety and Security (Centre for Applied Legal Studies Intervening) 2001 (4) SA 938 (CC).

Curtis v Minister of Safety and Security 1996 (3) SA 617 (CC).

Curtis v Minister of Safety and Security 2000 (10) BCLR 1079 (CC).

Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems Case C-311/18.

Dendy v University of the Witwatersrand, Johannesburg 2005 (5) SA 357 (W).

Dlomo v Natal Newspapers (Pty) Ltd 1989 (1) SA 945 (A).

*Dow Jones and Company Inc v Gutnick (*2002) 210 CLR 575.

Engels v Allied Chemical Manufacturers (Pty) Ltd 1993 (4) SA 45 (NM).

Ensor v Rensco Motors (Pty) Ltd 1981(1) SA 815 (A).

Epstein v Epstein 1906 TH.

Farrar's Estate v Commissioner's Case for Inland Revenue 1926 TPD 501.

Faydene Shirt 5 Clothing Manufacturers (Pty) Ltd v Levy 1966 (1) SA 26 (D).

Ferreira v Levin 1996 (1) SA 984 (CC).

Financial Mail (Pty) Ltd v Sage Holdings Ltd 1993 (2) SA 451 (A).

GC et al v CNIL (2019) C-136/17.

Gluitter v Lombard 2007 (2) RSA (SCA).

Google Spain SL v AEPD (the DPA) and Maria Costeja Gonzalez (2014) C-131/12, 13.5.

Gosschalk v Rossouw 1966 (2) SA 476 (C).

Grey v Pearson 1843-60 All ER Rep 21 (HL).

H v W 2013 2 All SA 218 (GSJ).

Harford Fire Insurance Co v Calfornia 1993 509 US 764.

Harksen v Lane 1998 (1) SA 300 (CC).

Hattingh v Roux 2011 (5) SA 135 (WCC).

Heroldt v Wills 2013 (2) SA 530 (GSJ).

Huey Extreme Club v Mc Donald t/a Sport Helicopters 2005 (1) SA 485 (C).

Hyundai Motor Distributors (Pty) Ltd v Smit 2001 (1) SA 545 (CC).

Inter-Science Research and Development Services (Pty) Ltd v Republica Popular de Mocambique 1980 (2) SA I 11(T).

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) Ltd v Smit 2001 (1) SA 545 (CC).

Janit v Motor Industry Fund Administrators (Pty) Ltd 1995 (4) SA 293 (A).

Jansen Van Vuuren v Kruger 1993 (2) All SA 619 (A).

Jooste v National Media Ltd 1994 (2) SA 634 (C).

Kaffraria Property Co (Pty) Ltd v Government of the Republic of Zambia 1980 (2) SA 709 (E).

Khumalo v Holomisa 2002 (5) SA 401 (CC).

Klein v Attorney-General, Witwatersrand Local Division 1995 (3) SA 848 (W).

Le Roux v Direkteur Generaal van Handel en Nywerheid 1997 (4) SA 174 (T).

Magajane v Chairperson North West Gambling Board 2006 (5) SA 250 (CC).

Magor & St Mellons Rural District Council v Newport Corporation 1950 2 All ER 1226 (CA) 1236

Masuku v Mdlalose 1998 (1) SA 1 (A).

Maximillian Schrems v Data Protection Commissioner, Case C- 362/14.

MEC for Health, Mpumalanga v M Net 2002 (6) SA 714 (T).

Mhlongo v Bailey 1958 (1) SA 885 (E).

Mhlongo v Minister of Police 1978 2 SA 551 (A).

Minister of Correctional Services v Tobani 2003 5 SA 126 (E).

Minister of Safety and Security v Van Duivenboden 2002 6 SA 431 (SCA).

Misty v Interim Medical and Dental Association of South Africa 1998 (4) SA 1127 (CC).

Mohamed and Another v President of the Republic of South Africa and Others (Society for the Abolition of the Death Penalty in South Africa and Another Intervening) 2001 (3) SA 893 (CC).

Morar v Casajee 1911 EDL.

Motor Industry Fund Administrators (Pty) Ltd v Janit 1994 (3) SA 56 (W).

National Coalition for Gay and Lesbian Equality v Minister of Justice 1999 (1) SA 6 (CC).

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

Nel v Le Roux 1996 (3) SA 562 (CC).

Ngwenyama v Mayelane 2012 (3) All SA 408 (SCA).

NM v Smith 2007 (5) SA 250 (CC).

O'Keeffe v Argus Printing and Publishing Co Ltd 1954 (3) SA 244 (C).

Pickard v SA Trade Protection Society 1905 (22) SC 89.

Powell v Van der Merwe 2005 (5) SA 62 (SCA).

Pretoria Portland Cement Co Ltd v Competition Commission 2003 (2) SA 385 (SCA).

Protea Technology Ltd v Winer 1997 (9) BLCR 1225 (W).

R v Holliday 1927 CPD 395.

R v Sutherland 1961 (2) SA 806 (A).

R v Sutherland 1961 (3) All SA 50 (A).

R v Umfaan 1908 TS 62.

Reid-Daly v Hickman 1981 (2) SA 315 (ZA).

Rhodesian Printing and Publishing Co Ltd v Duggan and Another 1975 (2) All SA 125 (RA).

S v A 1971 (2) SA 293 (T).

S v Bailey 1981 (4) SA 187 (W).

S v I 1976 (1) SA 781 (A).

S v Kruger 1968 (1) SA 484 (T).

S v Kruger 1968 (1) SA 507 (T).

S v Makwanyane 1995 (3) SA 391 (CC).

S v Mokgethi 1990 (1) SA 32 (A).

Schrems and Facebook Ireland v Data Protection Commissioner CJEU (2020) C-311/18.

Schrems v Data Protection Commissioner CJEU (2015) C-362/14.

Schuurman v Motor Insurers' Association of SA 1960 (4) SA 97 (T).

Sex Worker Education and Advocacy Task Force (SWEAT) v Minister of Safety and Security 2009 (6) SA 513 (WCC).

Shabalala Msimang v Sunday Times 2008 (6) SA 102 (W).

Shaw v Director of Public Prosecutions 1961 (2) All ER 446 (HL).

South Atlantic Islands Development Corporation Ltd v. Buchan 1971 (1) SA 234 (C).

SS Lotus France v SS Bozkourt Turkey 1927 PCIJ (ser A) No 10.

Steenkamp v Provincial Tender Board, Eastern Cape 2007 (3) SA 121 (CC).

Swanepoel v Minister van Veiligheid en Sekuriteit 1999 (4) SA 549 (T).

Thoroughbred Breeders Association v Prince Waterhouse 2001 (4) SA 551 (SCA).

Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy (2008) C-73/07

Tobani v Minister of Correctional Services 2002 (2) SA 318 (SEC).

Torwood Properties v SA Reserve Bank 1996 (1) All SA 215 (W).

United States v Alcoa 148 F2d 416 (2d Cir 1945).

United States v Microsoft Corp., No. 17-2, 548 U.S. 2018 WL 1800369.

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

Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk 1979 (1) SA 441 (A).

Van Eeden v Minister of Safety and Security 2003 (1) SA 389 (SCA).

Vryenhoek v Powell 1996 (1) BCLR 1 (CC).

Yahoo! Inc v La Ligue Contre Le Racisme Et L'A.ntisemiisme 433 F3d 1199 (9th Cir 2006).

Yahoo! Inc. v La Ligue Contre LeRacisme et L'Antisemitisme 169 F. Supp. 2d. 1181 (N.D. Cal. 2001) (No. 00-21275).

Books

A Huet and R Koering-Joulin *International Criminal Law* 3rd Edition (2005) University of France Press: Paris.

A Roos "Data Privacy" in D van de Merwe, S Eiselen and S Nel *Information and Communications Technology Law* 2nd Edition (2016) LexisNexis: South Africa.

B E Carter, P Trimble and A S Weiner *International Law* 5th Edition (2007) Aspen Publishers.

C Bennett and C Raab *The Governance of Privacy: Policy Instruments in Global Perspective* 1st Edition (2006) Cambridge Massachusetts Institute Technology Press: Massachusetts.

C D Wallace *The Multinational Enterprise and Legal Control: Host State Sovereignty in an Era of Economic Globalisation* 15th Edition (2002) Martinus Nijhoff: New York.

C Fombad *Constitutional Adjudication in Africa* (2017) Oxford University Press: South Africa.

C R Snyman *Criminal Law* 6th Edition (2008) LexisNexs: Butterworths Durban.

D Brand, C Gevers, K Govender, P Lenaghan, D Mailula, N Ntlama and S Sibanda *South African Constitutional Law in Context* 1st Edition (2014) Oxford University Press: South Africa.

D J McQuoid-Mason *The Law of Privacy in South Africa* (1978) LexisNexis: Butterworths: Durban.

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

E de Stadler and P Esselaar *A Guide to the Protection of Personal Information Act* 1st Edition (2015) Juta & Co Ltd: Cape Town.

E Steyn and A Nicol *Handbook of Trauma for Southern Africa* 5th Edition (2017) Oxford University Press.

G E Devenish *Interpretation of Statutes* 1st Edition (1992) Juta & Co Ltd: Cape Town.

G E Devenish *The South African Constitution* 3rd Edition (2005) Butterworths LexisNexis: Durban.

G Gilbert *Responding to International Crime* 2nd Edition (2006) Martinus Nijhoff: Brill.

H Donnedieu de Vabres *Treaty on Criminal Law and Comparative Law* 3rd Edition (1947) Sirey: Paris.

H H Hahlo and E Kahn *South African Legal System and its Background* (1969) Juta & Co Ltd: Cape Town (Published online by the University of Cambridge 17 January 2008).

H P Aust *Complicity and the Law of State Responsibility* (2011) Cambridge University Press: England.

I Currie and J de Waal *The Bill of Rights Handbook* 5th Edition (2005) Juta & Co Ltd: Cape Town.

I Currie and J de Waal *The Bill of Rights Handbook* 6th Edition (2013) Juta & Co Ltd: Cape Town.

I Justinian *The Digest of the Roman Law: Theft, Rapine, Damage and Insult* Reprint Edition (1979) Penguin Classics.

I M Rautenbach *Bill of Rights Compendium* 1st Edition (1996) Lexis Nexis: Butterworths Durban.

J Church, C Schulze and H Strydom *Human Rights from an International and Comparative Law Perspective* 6th Edition (2007) UNISA Press: Pretoria.

J Neethling, J M Potgieter and A Roos *Neethling on Personality Rights* 2nd Edition (2019) LexisNexis: Durban.

J Neethling, J M Potgieter and P J Visser *Law of Delict* 5th Edition (2006) Lexis Nexis: Butterworts Durban.

J Neethling, J M Potgieter and P J Visser *Neethling's Law of Personality* 2nd Edition (2005) Lexis Nexis: Butterworths Durban.

J Neethling, JM Potgieter and P J Visser *Law of Delict* 7th Edition (2014) Lexis Nexis: Butterworths Durban.

L M du Plessis *An Introduction to Law* 3rd Edition (1999) Juta & Co Ltd: Cape Town.

L M du Plessis *Re-Interpretation of Statutes* (2002) LexisNexis: South Africa.

M Foucault *Discipline and Punish: The Birth of the Prison* 2nd Edition (1995) New York Random House: New York.

M Loubser and R Midgley *The law of Delict in South Africa* 3rd Edition (2018) Oxford University Press: South Africa.

P De Vos and W Freedman *South African Constitutional Law in Context* 1st Edition: (2015) Oxford University: South Africa.

R Buyya, C Vecchiola and S T Selvi *Mastering Cloud Computing: Foundations and Applications Programming* (2013) Elsevier: New York.

R Cross *Statutory Interpretation* 3rd Edition (Revised) (1995) LexisNexis: Butterworth: Durban.
R J Midgley and JC Van der Walt *Principles of Delict* 4th Edition (2016) NexisLexis Butterworth: Durban.
S R Smoot and N K Tan *Private Cloud Computing: Consolidation, Virtualization, and Service-Oriented Infrastructure* 1st Edition (2011) Elseiver.
S Snail and S Papadopoulos *Cyberlaw @SA III: The Law of Internet in South Africa* 3rd Edition (2012) Van Schaick Publishers: Pretoria.
S Woolman, T Roux and M Bishop *Constitutional Law of South Africa* 2nd Edition (2008) Juta & Co Ltd: Cape Town.
South African School Dictionary 3rd Edition (2010) Oxford University Press: South Africa.

Theses and dissertations

A Naude *Data Protection in South Africa: The Impact of the Protection of Personal Information Act and Recent International Developments* (LLM Mini-Dissertation, UP, 2014).
A P Jackson *Legal Concerns Arising from the Use of Cloud Technologies* (LLD Thesis, UP, 2017).
A Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (LLD Thesis, UNISA, 2009).
A Singh *The Impact of the Constitution on Transforming the Process of Statutory Interpretation in South Africa* (LLD Thesis, UKZN, 2014).
R Ahmed *The Explicit and Implicit Influence of Reasonableness on the Elements of Delictual Liability* (LLD Thesis, UNISA, 2018).
S E Mokowadi-Tladi *The Regulation of Unsolicited Electronic Communication(Spam) in South Africa: A Comparative Study* (LLD Thesis, UNISA, 2017).

Journals and Articles

A B Vickery “Breach of Confidence: An Emerging Tort” (1982) 82(7) *Columbia Law Review* 1428.
A Cormack “Incident Response: Protecting Individual Rights under the General Data Protection Regulation” (2016) 13 *SCRIPTed* 258.

A D Mitchell and J Hepburn “Don’t Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer” (2017) 19 *Yale Journal of Law and Technology* 182.

A Deb “Cyber Crime and Judicial Response in India” (2012) 3 *Indian Journal of Law and Justice* 106.

A F Westin “Privacy and Freedom” (1967) 25(1) *Washington and Lee Law Review* 166.

A L D Pereira “Cloud Computing” (2017) 93 *Bol. Fac. Direito U. Coimbra* 89.

A Naude and S Papadopoulos “Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments (Part 1)” (2016) *THRHR* 51.

A Roos “Core Principles of Data Protection Law” (2006) 39 *CILSA* 102.

A Roos “Explaining the International Backdrop and Evaluating the Current South African Position” (2007) 124 *SALJ* 2.

A Roos “Personal Data Protection in New Zealand: Lessons for South Africa” (2008) 4 *Potchefstroom Electronic Law Journal* 62.

A Roos “Privacy in the Facebook Era: A South African Legal Perspective” (2012) 129 *South African Law Journal* 375.

A Roos “The European Union’s General Data Protection Regulations (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected ‘Content Principles’” (2020) 53(3) *Comparative and International Law Journal of Southern Africa* 1.

A S Perrin “The General Data Protection Regulation and Open Source Software Communities” (2021) 12 *Cybaris INTELL. PROP. L. REV.* 77.

A Savoiu and C C Basarabescu “The Right to Privacy” (2013) *Annals Constantin Brancusi U. Targu Jiu Juridical Sci. Series* 89.

A Schildhaus “EU’s General Data Protection Regulation GDPR: Key Provisions and Best Practices” (2017) 46 *INT’l L. News* 12.

A Solow-Niederman “Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches” (2017 to 2018) 127 *Yale Law Journal Fisher* 614.

A von dem Bussche-Freiherr and A Zeiter “Implementing the EU General Data Protection Regulation: A Business Perspective” (2016) 2 *European Data Protection Law Review* 576.

C Kuner “An International Legal Framework for Data Protection: Issues and Prospects” (2009) 25 *Computer law and Security Review* 307.
C Kuner “Data Protection Law and International Jurisdiction on the Internet (Part 1)” (2010) 18 (2*) International Journal of Law and Information Technology* 176.
C Kuner “The European Union and the Search for an International Data Protection Framework” (2009) 2(2) *GroJIL* 55.
C M van der Bank “The Right to Privacy-South African and Comparative Perspective” (2012) 1(6) *European Journal of Business and Social Sciences* 77.
C Okpaluba “Constitutional Protection of the Right to Privacy: The Contribution of Chief Justice Langa to the Law of Search and Seizure” (2015) *ACTA JURIDICA* 407.
C Reed *“*Information Ownership in the Cloud” (2009) Research Paper No 45/2010 *Queen Mary University of London, School of Law, Legal Studies*.
C S D Brown “Investigating and Prosecuting Cybercrime: Forensic Dependencies and Barriers to Justice” (2015) 9(1) *International Journal of Cyber Criminology* 55.
C Sullivan “Protecting Digital Identity in the Cloud: Regulating Cross Border Data Disclosure” (2014) 30 *Computer Law & Security Review* 137.
C Yav “Perspective on the GDPR from South Africa” (2018) 2 *International Journal Data Protection Officer, Privacy Officer and Privacy Counsel* 19.
D A Couillard “Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing” (2009) 93 *Minnesota Law Review* 2205.
D C Andrews and J M Newman “Personal Jurisdiction and Choice of Law in the Cloud” (2013) 73 *Md. L. Rev*. 313.
D H Flaherty “On the Utility of Constitutional Rights to Privacy and Data Protection” (1991) 41 *Case Western Reserve Law Rev*iew 831.
D J Davies “Criminal law and the Internet: The Investigator’s Perspective: Crime, Criminal Justice and the Internet” (1998) *Criminal Law Rev Special Edition* 1.
D J McQuoid-Mason “Invasion of Privacy: Common Law v Constitutional Delict – Does it Make a Difference?” (2000) *Acta Juridica* 236.
D K Citron “Mainstreaming Privacy Torts” (2010) 98 *University of California Law Review* 1805.
D Manescu “Recovery of Claims in the GDPR (General Data Protection Regulation) Era” (2018) 8 *JURIDICAL TRIB* 789.

D Millard and E G Bascerano “Employers’ Statutory Vicarious Liability in Terms of the Protection of Personal Information Act (2016) 19 *Potchefstroom Electronic Law Journal* 1.

E F Ryan “Privacy, Orthodoxy and Democracy” (1973) 51 *Canadian Bar* 84.

E O’Dell “Compensation for Breach of the General Data Protection Regulation” (2017) 40 *DUBLIN U. L.J.* 97.

E Volokh “Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You” (2000) 52 *Stanford Law Review* 1049.

F Gilbert “Proposed EU Data Protection Regulation: The Good, the Bad and the Unknown” (2012) 15(10) *Journal of Internet Law* 1.

F Pasquale and T A Ragone “Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing” (2014) 17 *Stanford and Technology Law Review* 595.

F Talat “Cyber Crimes: Challenging the Paradigms of Traditional Criminal Law” (2005) 3 *Corporate Law Cases* 475.

F Tasneem “Electronic Contracts and Cloud Computing” (2014) 9(2) *Journal of International Commercial Law and Technology* 105.

G Carlson, J McKinney, E Slezak and E S Wilmot “General Data Protection Regulation and California Consumer Privacy Act: Background” (2020) 24 *Currents Journal of International Economic Law* 62.

G E Coffield “Love Hurts: How to Stop the Next ‘Love Bug’ From Taking a Bite Out of Commerce” (2001) 20 *Journal of Law and Commerce* 254.

G Gilbert “Crimes Sans Frontières: Jurisdictional Problems in English Law” (1993) 63(1) *British Yearbook of International Law* 1.

G Hyman “The Concept of Privacy” (1967) 42 *New York University Law Review* 34.

G Spindler and P Schmechel “Personal Data and Encryption in the European General Data Protection Regulation” (2016) 7 *J. INTELL. PROP. INFO. TECH. & ELEC. COM. L.* 163.

H B Jr Dixon “Cloud Computing” (2012) 51(2) *Judges Journal* 36.

H Gross “The Concept of Privacy” (1967) 42 *NYULR* 34.

H Lobel “Cyber War Inc.: The law of war implications of the private sectors role in cyber conflict” (2012) 47 *Texas International Law Journal* 617.

H T M Nguyen “Cloud Cover: Privacy Protections and the Stored Communications Act in the Age of Cloud Computing” (2011) 86 *Notre Dame Law Review* 2189.

I Alexe “The Sanctioning Regime Provided by Regulation (EU) 2016/679 on the Protection of Personal Data” (2018) *INT’L LAW REVIEW* 60.

I M Rautenbach “The Conduct and Interests Protected by the Right to Privacy in Section 14 of the Constitution” (2001) *TSAR* 116.

Information Regulator of South Africa Guidance Note on the Processing of Personal Information in the Management and Containment of Covid-19 Pandemic in terms of the Protection of Personal Information Act 4 of 2013 (POPI Act) (3 April 2020) Privacy Guidance 2.2.2. https://www.justice.gov.za/ (Accessed 27 January 2021).

J A Muir and PC Van Oorschot “Internet Geolocation and Evasion” (2009) 4 *ACM Computer Survey* 1.

J A Stiven “Preparing and Advising Your Clients on Cloud Usage” (2014) 12 (4) *De Paul Bus and Commercial Law Journal* 421.

J B Maillart “The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime”(2018) 19 *ERA Forum* 378 to 379 https://doi.org/ 101007s12027-018-0527-2 (Accessed 12 July 2020).

J Burchell “The Legal Protection of Privacy in South Africa: A Transplantable Hybrid” (2009) 13 *Electronic Journal of Comparative Law* http://www.unuvu.eicl.oig (Accessed 10 August 2020).

J C Nelson “Keynote Addresses: The Right to Privacy” (2007) 68 *Montana Law Review* 257.

J Clarke “The Regulation of Civilian Drones’ Impact on Behavioural Privacy” (2014) *Computer and Security Law Review* 287.

J Dumas “General Data Protection Regulation (GDPR): Prioritizing Resources” (2019) 42 *Seattle U. L. REV.* 1115.

J G McCarthy “The Passive Personality Principle and Its Use in Combating International Terrorism” (1989) 13(3) *Fordham International Law Journal* 298.

J Greene “Beyond Lawrence: Metaprivacy and Punishment” (2006) 115 *Yale Law Journal* 1862.

J Litman “Information Privacy/Information Property” (2000) 52 *Stanford Law Review* 1283.

J Neethling “Features of the Protection of Personal Information Bill, 2009 and the Law of Delict” (2012) 75 *THRHR* 241.

J Neethling “Personality Rights: A Comparative Overview” (2005) 38 *Comparative and International Law Journal of South Africa* 210.
J Neethling “The Concept of Privacy in South African Law” (2005) 122 *South African Law Journal* 18.
J Neethling “The Constitutional Court Gives the Green Light to the Common Law of Defamation” (2002) 119 *South African Law Journal* 700.
J Neethling “The Protection of the Right to Privacy Against Fixation of Private Facts” (2004) 121 *South African Law Journal* 519.
J Neethling “The Right to Privacy, HIV/AIDS and Media Defendants” (2008) 125 *South African Law Journal* 36.
J Neethling “Tort law in South Africa - The Mixing of the General and the Particular” (2001) *The Contribution of Mixed Legal Systems to European Private Law* 81.
J R Reidenberg “*Lex Informatica*: The Formulation of Information Policy Rules Through Technology” (1998) 76 *TEX. L. Rev.* 553.
J Ryan “The Uncertain Future: Privacy and Security in Cloud Computing” (2014) 54(2) *Santa Clara Law Review* 497.
J Zittrain “Response, Engineering an Election: Digital Gerrymandering Poses a Threat to Democracy” (2014) 127 *Harvard Law Review* 335.
K Allan and I Currie “Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa” (2007) 23 *South African Journal on Human Rights* 570.
K Feng and S Papadopoulos “Student (K-12) Data Protection in the Digital Age: A Comparative Study” (2018) 51 *Comparative and International Law Journal of Southern Africa* 261.
K Gormley “One Hundred Years of Privacy” (1992) *Wisconsin Law Review* 1335.
K Hixson “Extraterritorial Jurisdiction Under the Third Restatement of Foreign Relations Law of the United States” (1988) 12(1) *Fordman International Law Journal* 127.
K N Rashbaum, B B Borden and T H Beaumont “Outrun the Lions: A Practical Framework for Analysis of the Legal Issues in the Evolution of Cloud Computing” (2014) 12(1) *AMLR* 71.
K Van der Schyff and K Krause “Higher Education and Cloud Computing in South Africa: Towards Understanding Trust and Adoption Issues” (2014) 55 *South African Computer Journal* 40.

L M du Plessis “Theoretical (Dis-) position and Strategic Leitmotivs in Constitutional Interpretation in South Africa” (2015) 18(5) *Potchefstroom Electronic Law Journal* 1332.

L Oprysk “The Forthcoming General Data Protection Regulation in the EU” (2016) 24 *JURIDICA INT’l* 23.

L Swales “Protection of Personal Information: South Africa’s Answer to the Global Phenomenon in the Context of Unsolicited Electronic Messages (Spam)” (2016) 28 *South African Mercantile Law Journal* 49.

M A Manuputty, S M Noor and J Sumardi “Legal’s Standing of Cyber Crime in International Law Contemporary” (2014) 22 *Journla of Law Policy and Globalization* 128.

M A Reetz, L B Prunty, G S Mantych and D J Hommel “Cyber Risks: Evolving Threats, Emerging Coverages, and Ensuing Case Law” (2018) 122 *Penn State Law Review* 727.

M Balkin “Information Fiduciaries and the First Amendment” (2016) 49 *University California Davis Law Review* 1183.

M Barbaro “Government Interference with the Right to Privacy: Is the Right to Privacy an Endangered Animal” (2017) 6 *Canadian Journal of Human Rights* 127.

M de Bruyn “The Protection of Personal Information (POPI) Act - Impact On South Africa” (2014) 13(6) *International Business and Economics Research Journal* 1325.

M H Greenberg “A Return of Lilliput: The *LICRA v Yahoo!* Case and the Regulation of Online Content in the World Market” (2003) *Berkeley Technology Law Journal* 1191.

M Hayashi “Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace” (2006) 6 *International Law Journal* 254.

M Laubscher and W J van Vollenhoven “Cyberbullying: Should Schools Choose Between Safety and Privacy” (2015) 18 *Potchefstroom ELEC. L.J.* 2218.

M Peihani “Financial Regulation and Disruptive Technologies: The Case of Cloud Computing in Singapore” (2017) *Singapore Journal of Legal Studies* 77.

M Reimann “The End of Comparative Law as an Autonomous Subject” (1996) 11 *Tulane European and Civil Law Forum* 49.

M Rosentau “The General Data Protection Regulation and Its Violation of EU Treaties” (2018) 27 *JURIDICA INT’l* 36.

M Singh and S Singh “Cyber Crime Convention and Trans Border Criminality” (2007) 1 *Masaryk University Journal of Law and Technology* 53.

M Szydfo “The Independence of Data Protection Authorities in EU Law: Between the Safeguarding of Fundamental Rights and Ensuring the Integrity of the Internal Market” (2017) 41 *European Law Review* 369.

N A Sales “Regulating Cyber-Security” (2012) 107 *Northwestern University Law Review* 1503.

N Baloyi and P Kotze “Are Organisations in South Africa Ready to Comply with Personal Data Protection or Privacy Legislation and Regulations?” (2017) *International Information Management Corporation* 1 http://www.ist-africa.org /Conference2017 (Accessed 31 May 2020).

N M Richards “The Limits of Tort Privacy” (2011) 9 *Journal of Telecommunications and High Technology Law* 357.

N Mashinini “The Processing of Personal Information Using Remotely Piloted Aircraft Systems in South Africa” (2020) 53 *De Jure Law Journal* 140.

N Olorunju *“*Security: The Protection of Personal Information in the Health Care System” (2019) 54 *Journal of Public Administration* 363.

N Seitz “Trans Border Search: A New Perspective in Law Enforcement” (2005) 7(1) *Yale Journal of Law Technology* 24.

N Shaik-Peremanov “Basel II - The Right to Privacy: A South African Perspective” (2009) 21 *South African Mercantile Law Journal* 546.

O Tambou “Lessons from the First Post-GDPR Fines of the CNIL Against Google LLC” (2019) 5 *EUR. DATA PROT. L. REv.* 80.

P Blume “EU Adequacy Decisions: The Proposed New Possibilities” (2015) 5 *IDPL* 34.

P Gabriel “The Protection of Personal Information Act 4 of 2013 and Children’s Right to Privacy in the Context of Social Media” (2019) 82 *THRHR* 605.

P L C Torremans “Extraterritorial Application of E.C and U.S. Competition Law” (1996) 21 *European Law Review* 1.

P Lanois “Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy” (2010) 9 *North-Western Journal of Technology and Intellectual Property* 29.

P M Schwartz “Property, Privacy, and Personal Data” (2004) 117 *Harvard Law Review* 2055.

P Rosenzweig “Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World” (2013) *Santa Barbara Praeger Security International* 78.

P Sahoo and T Jaiswal “Cloud Computing and its Legalities in India” (2014) 4 *Nirma University Law Journal* 65.

R Berry and M Reisman “Policy Challenges of Cross-Border Cloud Computing” (2012) 4 *Journal of International Commerce and Economics* 1.

R Broadhurst “Developments in the Global Law Enforcement of Cyber-Crime” (2006) 29 *An International Journal of Police Strategies and Management* 408.

R H Carpenter Jr “Walking from Cloud to Cloud: The Portability Issue in Cloud Computing” (2010) 6 *Washington Journal of Law Technology and Arts* 1.

R Sony “Implications of Cloud Computing for Personal Data Protection and Privacy in the Era of the Cloud: An Indian Perspective” (2013) *Law Journal of Higher School of Economics* 3.

R Telang “Policy Framework for Data Breaches” (2015) 13 *IEEE Security and Privacy* 77.

R Uerpmann-Wittzack “Principles of International Internet Law” (2010) 11 *German Law Journal* 1245.

R von Solms and M Viljoen “Cloud Computing Service Value: A Message to the Board*”* (2012) 43(4) *Journal of Business Management* 73.

Research in International Law Under the Auspices of the Faculty of the Harvard Law School “Jurisdiction with Respect to Crime” (1935) 29 *American Journal of International Law* 443.

S Bhaimia “The General Data Protection Regulation: The Next Generation of EU Data Protection” (2018) 18 *LIM* 21.

S Bradshaw, C Millard and I Walden “Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services” (2011) 19(3) *International Law Journal and Information Technology* 187.

S C Rickless “The Right to Privacy Unveiled” (2007) 44 *San Diego Law Review* 773.

S Huneberg “On drones, New Risk and Insurance” (2017) *THRHR* 586.

S L Hoppkins “Cyber Crime Convention: A Positive Beginning to a Long Road Ahead” (2003) 2 *Journal of High Technology Law* 102.

S L Howard “The Web That Binds Us All: The Future of Legal Environment of the Internet” (1997) 19 *Houston Journal of International Law* 501.

S M Gilles “Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy” (1995) 43 *Buffalo Law Review* 1.

S M Puiszis “Unlocking the EU General Data Protection Regulation” (2018) *J. PROF.LAW.* 1.
S Mutkoski “Cloud Computing, Regulatory Compliance, and Student Privacy: A Guide for School Administrators and Legal Counsel” (2014) 30 *John Marshall Journal of Information Technology and Privacy Law* 511.
S Sean “Governing Cyberspace: The Need for an International Solution” (1997) 32 *Gonzalez Law Review* 376.
S W Brenner “Toward a Criminal Law for Cyberspace: Product Liability and Other Issues” (2004) 1 *Pittsburgh School of Law Journal of Technology Law* 1.
S Warren and L Brandeis “The Right to Privacy” (1890) 4 *Harvard Law Review* 193.
S Wilske and T Schiller “International Jurisdiction in Cyberspace: Which States May Regulate the Internet?” (1997) 50 *Federal Communications Law Journal* 117.
S Yakovleva and K Irion “Toward Compatibility of EU Trade Policy with the General Data Protection Regulation” (2020) 114 *AJIL UNBOUND* 10.
S Zimmeck “The Information Privacy Law of Web Applications and Cloud Computing” (2012) 29 *Santa Clara Computer & High Technology Law Journal* 451.
T D Martin “Hey! You! Get Off My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security and Property in Cloud Computing” (2010) *Journal of the Patent & Trademark Office Society Selected Works* https://works.bepress.com (Accessed 21 March 2020).
T H Beaumont “Outrun the Lions: A Practical Framework for Analysis of the Legal Issues in the Evolution of Cloud Computing” (2014) 12(1) *AMLR* 71.
T N Foster “Navigating Through the Fog of Cloud Computing Contracts” (2013) 30(1) *The John Marshall Journal of Information Technology and Privacy Law* 13.
T Peterson “Cloudy with a Chance of Waiver: How Cloud Computing Complicates the Attorney-Client Privilege” (2012) 46 *J Marshall L Rev* 383.
T Riley “Privacy and Data Protection: An International Bibliography” (1986) 7 *Journal of Media Law and Practice* 77.
T Takahashi “Drones and Privacy” (2012) 14 (1) *Columbia Science and Technology Law Report* 72.
U Joshi “Online Privacy and Data Protection in India: A Legal Perspective” (2013) 7 *NUALS Law Journal* 95.

U Sieber and C W Neubert “Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty” (2017) *Max Planck Yearbook of United Nations Law* 257.

V Narayanan “Harnessing the Cloud: International Law Implications of Cloud-Computing*”* (2012) 12 *Chicago Journal of International Law* 783.

V Shetty “Computing the Tax on Cloud Computing” (2014) 8 *Law Review Government Law College* 159.

W A Parent “Privacy, Morality, and the Law” (1983) 12 *Phil. and Pub. Aff.* 269.

W G Voss “Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation” (2016) 50 *R.J.T. n.s.* 783.

W G Voss “Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later” (2014) 17 *J. INTERNET L.* 1

W G Voss and H Bouthinon-Dumas “EU General Data Protection Regulation Sanctions in Theory and in Practice” (2020) 37 *Santa CLARA HIGH TECH. L. J*. 1.

W Hartzog “Reviving Implied Confidentiality” (2014) 89 *Indiana Law Journal* 763.

W K Hon and C Millard “Cloud Technologies and Services” (2013) *Cloud Computing Law Oxford: Oxford University Press* 3.

W K Hon, C Millard and I Walden “Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now” (2012) 16 (1) *Stanford and Technology Law Review* 79.

W K Hon, C Millard and I Walden “The Problem of ‘Personal Data’ in Cloud Computing: What Information is Regulated? The Cloud of Unknowing” (2011) 1(4) *IDPL* 211.

W K Hon, J Hornle and C Millard *“*Data Protection Jurisdiction and Cloud Computing: When Are Cloud Users and Providers Subject to EU Data Protection Laws? The Cloud of Unknowing” (2012) 26(2-3) *International Review of Law Computers and technology* 129.

Y Onn “Privacy in Digital Environment” (2005) 7 *Haifa Centre of Law and Technology* 1.

Internet sources

"The History of Yahoo-How It All Started" *Yahoo! Media Relations* http://docs.yahoo.comlinfo /misclhistory.html (Accessed 02 July 2020).

A C Krikos "Cloud Computing as a Disruptive Technology" (2011) http://www.media.cloudbook.net (Accessed 03 July 2020).

A Gillwald, M Moyo and M Altman "Cloud Computing in South Africa: Prospects and Challenges" (2012) https://www.researchgate.net/publication/331639595 (Accessed 30 May 2020).

A Monaco "A View Inside the Cloud*"* (7 June 2012) *The Institute IEEE Spectrum* http://theinstitute.ieee.org (Accessed 03 July 2020).

Abraham and Gross Attorneys, Notaries and Conveyances "Vicarious Liability and What It Means for Employers" (14 November 2017) *Criminal Law, Labour and Employment Litigation and Dispute Resolution* https://www.abgross.co.za/vicarious-liability-and-employers/ (Accessed 25 February 2022).

Amazon EC2 Amazon Web Services http://aws.amazon.com / (Accessed 04 July 2020).

Amazon Web Services "Airbnb Case Study" https://www.amazon.com/solutions/case-studies/airbnb/ (Accessed 03 July 2020).

American Institute Restatement of the Law Third: The Foreign Relations Law of the United States http://www.ali.org/publications/show/foreign-relatios-law-united-states-rest/ (Accessed 09 April 2020).

Art. 46 nouv. C. pr. civ, English translation https://www.legifrance.gouv.fr/content/download/1962/13735/version/3/.../Code_39.pdf (Accessed 10 July 2020).

Article 29 *Data Protection Working Party* 01037/12/EN WP 196 Opinion 5/2012 on Cloud Computing (2012) 4 http://ec.europa.eu/justice/data-protection/index_en.htm (Accessed 21 March 2020).

B Fung "After the Equifax Breach, Here's How To Freeze Your Credit To Protect Your Identity" (9 September 2017) *Washington Post* http://www.washingtonpost.com/news/the-switch/wp/2o17/o9/o9/ (Accessed 10 August 2020).

B Preston "Customers Fire a Few Shots at Cloud Computing" (16 Jun 2008) *INFO WK* http://www.informationweek.com/news/services/data/ (Accessed 04 April 2020).

B Smith "Cloud Computing for Business and Society at the Brookings Institution" (2010) *Brookings Institution* http://www.brookings.edu / (Accessed 07 April 2020).

C Cooper “The Cloud Drives a New Wave of Disruption” (25 June 2015) *CIO* http://www.cio.com/article/2940519/cloud-infrastructure/the-cloud-drives-a-new-wave-of-disruption.html (Accessed 03 July 2020).

C Dolley “Cyberattacks: South Africa, You’ve been Hacked” (6 November 2021) *Daily Maverick* https://www.dailymaverick.co.za/article/2021-11-06-cyberattacks-south-africa-youve-been-hacked/ (Accessed 24 February 2022).

D McGinnis “What is the Industrial Revolution?” (27 October 2020) *the 360 blog* https://www.salesforce.com/blog/what-is-the-fourth-industrial-revolution-4ir/ Accessed 26 February 2022)

E Dou “Is Europe Ready to Put Its Data in the Clouds?” (27 April 2011) *AI Brand Channel=0* http://af.reuters.com/article/ethiopiaNews/ (Accessed 04 April 2020).

E Dou “Is Europe Ready to Put Its Data in the Clouds?” (27 April 2011) *AI Brand Channel=O* 1 http://af.reuters.com/article/ethiopiaNews/ idAFLDE7341NU20110426 (Accessed 04 April 2020).

E McCormick “Is Banking’s Future in the Cloud?” (12 September 2012) *BankDirector.com* http://www.bankdirector.com/ (Accessed 04 July 2020).

E Pirkova and E Masser “The EU Court decides on two major “right to be forgotten” cases: there are no winners here” (23 October 2019) *Accessnow* https://www.accessnow.org/eu-court-decides-on-two-major-right-to-be-forgotten-cases-there-are-no-winners-here/ (Accessed 09 August 2021).

Forcepoint https://www.forcepoint.com/cyber-edu/spoofing (Accessed 21 February 2022).

French Criminal Penal Code of 2005 01/01/2005 https://www.legal-tools.org /doc/418004.CODE PENAL [C. PEN.] art. R.645-1 (Fr.) English Translation http://www.lex2k.org/yahoo/ art645.pdf (Accessed 11 July 2020).

G Vladimir “International Cooperation in Fighting Cyber Crime” (2005) *Crime Research* http://www.crime-research.org (Accessed 02 July 2020).

GDPR FAQs: Frequently Asked Questions About GDPR, EU GDPR.ORG https://eugdpr.org/the-regulation/gdpr-faqs/ https://perma.cc/3WBX-EEE4 (Accessed 07 August 2021).

Google only has data servers located in some parts of the Americas, Asia and Europe, but not Africa while many of its users are in Arica as well https://www.google.com/about/datacenters/inside/locations/ (Accessed on 30 March 2020).

H F Lipson “Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues” (2002) *Carnegie Mellon Software Engineering Institute* https://resources.sei.cmu.edu/asset_files/SpecialReport/2002_003_001_13928.pdf (Accessed 11 July 2020).

H Marshall-Jarrett, M W Bailie and E Hagen *“*Prosecuting Computer Crime” (2010) *Office of Legal Education: Executive Office of U. S. Attorneys* http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14 (Accessed 10 August 2020).

Information Regulator (IR) South Africa “Information Regulator’s IT Systems Affected by a Ransomware Attack on the Department of Justice & Constitutional Development” (13 September 2021) *Media Statement* https://www.justice.gov.za/inforeg/docs/ms/ms-20210913-ITsystems.pdf (Accessed 24 February 2022) and

Information Regulator of South Africa: Amended Notice Relating to Amended Guidelines to Develop Codes of Conduct in terms of Chapter 7 of the Protection of Personal Information Act of 2013 3 https://www.justice.gov.za/inforeg/docs/20181214-gg42110-rg10897-gon1383-POPIregister pdf (Accessed 02 March 2021).

Information Systems Audit and Control Association “IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud” (2011) *ISACA* http://www.isaca.org/ (Accessed 05 July 2020).

Invitation to submit written submissions on the proposed National Data and Cloud Policy: Government gazette Number 309 (44411) (1 April 2021) http//:www.gpwonline.co.za 3 (Accessed 14 May 2021).

Invitation to submit written submissions on the proposed National Data and Clod Policy: Government gazette Number 309 (44411) (1 April 2021) http//:www.gpwonline.co.za 3 (Accessed 14 May 2021).

IT Governance Network “Impact of the POPI Act on Cloud Computing” (2013) http://www.itgovernance.co.za (Accessed 10 March 2021).

J Coleman, S Hershovitz and G Mendlow “Theories of the Common Law of Tort” (2015) *Stanford Encyclopaedia of Philosophy* https://plato.stanford.edu/entries/tort-theories/ (Accessed 22 August 2020).

J Hage and J S Brown “Cloud Computing - Storms on the Horizon” *Deloitte Centre for the Edge* http://www.johnseelybrown.com/cloudcomputingdisruption.pdf (Accessed 05 July 2020).

J J Schwerha “Law: Law Enforcement Challenges in Trans-border Acquisition of Electronic Evidence from Cloud Computing Providers” (2010) *Council of Europe Discussion Paper* https://rm.coe.int/16802fa3dc (Accessed 10 July 2020).

J M Balkin “Information Fiduciaries in the Digital Age” (5 March 2014) *Balkinization* http://balkin.blogspot.com/2o14/o3/ (Accessed 09 August 2020).

J McKendrick “Cloud Computing Market Hot, but How Hot? Estimates are All Over the Map” (13 February 2012) *Forbes* http://www.forbes.com/ (Accessed 07 July 2020).

J N Hoover and R Martin “Demystifying the Cloud” (23 June 2008) *INFO WK* http://www.informationweek.com/news/services/ (Accessed 04 April 2020).

J Orr “City of Johannesburg Announces Second Ransomware Attack in Recent Months” (24 October 2019) *Cyber Security Hub* https://www.cshub.com/attacks/articles/city-of-johannesburg-announces-second-ransomware-attack-in-recent-months (Accessed 28 September 2021).

J P Meltzer “The Court of Justice of the European Union in Schrems II: The Impact of the GDPR on Data Flows and National Security” (5 August 2020) *Brookings* https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/#footnote-1 (Accessed 09 August 2020).

J Q Anderson and L Rainie “The Future of Cloud Computing” (11 June 2010) *PEW Internet and American Life Project* http://pewresearch.org/pubs/1623/ (Accessed 25 July 2020).

J Sluijd, P Larouche and W Sauter “Cloud Computing in the EU Policy Sphere Interoperability, Vertical Integration and the Internal Market” (2012) *Tilburg Law and Economics Center (TILEC)* https://www.jipitec.eu/ (Accessed 04 April 2020).

K Shaw “What is IPv6 and Why Are We Not There Yet?” (27 September 2018) *Network World* https://www.networkworld.com (Accessed 12 July 2020).

M A Dennis “Cybercrime Law” *Britannica* https://www.britannica.com/topic/cybercrime (Accessed 23 February 2022).

M Peihan “Let It Rise: A Special Report on Corporate IT” (2008) *The Economist* 3 http://the.economist.com /node/12411882 (Accessed 03 July 2020).

M V P Asinari “The WTO and the Protection of Personal Data. Do EU Measures Fall Within GATS Exception? Which Future for Data Protection within the IVTO E-Commerce Context?” (2003) *18th BILETA Conference* http://www.bileta.ac.uk/ (Accessed 04 July 2020).

Marsh and Mclennan companies “Dawning of the Drones: The Evolving Risk of Unmanned Aerial Systems” (2015) *Marsh* http://www.bit.ly/2nXQQoO (Accessed 2 December 2020).

N S Gil “What is the Sword of Damocles?, Classical history” http://ancienthistory.about.com (Accessed 30 May 2020).

Nelson Mandela, South African Former President and Civil rights Activist (updated 30 October 2015) *UCT Amnesty International* http://www.amnesty.org (Accessed 18 July 2020).

NRO “Regional Internet Registries” https://www.nro.net (Accessed 12 July 2020).

P De Vos “South African Constitutional Law in Context” (2014) *Research Gate* https://www.researchgate.net/publication/266031366 (Accessed 17 July 2021).

P Mell and T Grance “ The NIST Definition of Cloud Computing” (2011) *U.S. Dept. of Commerce National Institute of Standards and Tech Special Publication No. 800-145, The NIST* http://csrc.nist.gov/publications/nistpubs/800-145/SP800- 145.pdf (Accessed 19 April 2020).

P S Mvelase, I Z Dlamini, H M Sithole and N Dlodlo “Towards a Government Public Cloud Model. The Case of South Africa (3 to 5 June 2013) *Cluster Computing Conference Paper* 149 http://hpc-ua.org/cc-13/files/proceedings/33.pdf (Accessed 7 July 2020).

Press Release “Fortify: Survey Reveals Vast Scale of Cloud Hacking - And the Need to Bolster Security to Counter the Problem” (2010) *Press Release, Fortify Software, DEF CON* https://www.globalsecuritymag.fr/ (Accessed 20 July 2020).

R Berry and M Reisman “Policy Challenges of Cross-Border Cloud Computing” (2012) *Journal of International Commerce and Economics*: United States International Trade Commission https://www.usitc.gov (Accessed 06 July 2020).

R Cohen “The Cloud Hits the Mainstream. More than Half of the US Businesses Now Use Cloud Computing” (16 April 2013) *Forbes* http://www.forbes.com/sites/reuvencohen (Accessed 09 April 2020).

R Luck “Is South Africa Keeping Up with International Trends?” (22 May 2013) *DEREBUS* http://www.saflii.org/za/journals/DEREBUS/2014/84.pdf (Accessed 12 March 2020).

R Luck “POPI- Is South Africa Keeping Up with International Trends?” (1 May 2014) *De Rebus* http://www.derebus.org.za/popi-south-africa-keeping-international-trends/ (Accessed 12 March 2020).

R Nichols “Cloud Computing by the Numbers: What do All the Statistics Mean?” (31 August 2010) *Computer Worl*d http://blogs.computerworld.com (Accessed 07 July 2020).

RIPE Network Coordination Centre https://www.ripe.net/ (Accessed 12 July 2020).

S D Abraham, J D Steinbruner, S M Bellovin, S Dycus, S E Brown, J L Goldsmith III, R Jervis, J M Lodal and P Venables “A Proposal for an International Convention on Cyber Crime and Terrorism” (2002) *The National Academies Press* http://www.iwar.org.uk/law/ (Accessed 01 July 2020).

S G Bradbury “Keynote Address: Law, Privacy, and Warfare in a Digital World” (2011) *Harvard National Security Journal Symposium: Cybersecurity* http://harvardnsj.com/ (Accessed 27 June 2020).

S Hoog and E Vyncke “Introduction to IPv6” (19 December 2008) *Cisco Press* https://www.networkworld.com (Accessed 12 July 2020).

S Keane “GDPR: Google and Facebook Face up to $9.3B in Fines on First Day of New Privacy Law” (25 May 2018) *CNET* https://www.cnet.com/news/gdpr-google-and-facebook-faceup-to-9-3-billion-in-fines-on-first-day-of-new-privacy-law (Accessed 02 July 2021).

S Robert “Privacy, Technology and National Security, An Overview of Intelligence Collection” (2013) *Office of the Director on National Intelligence, Brookings Institution* https://www.dni.gov/index.php/ (Accessed 21 January 2021).

SunTrust Banks “Improving Productivity, Reducing Vulnerability Windows” (25 February 2011) *International Business Machines Corp (IBM)* http://www-03.ibm.com (Accessed 04 July 2020).

T Gonen “Data Breach Prevention is Dead” (9 February 2015) Hill http://thehill.com/blogs/congress-blog/technology/ (Accessed 09 August 2020).

T Hsu “Data Breach Victims Talk of Initial Terror, Then Vigilance” (9 September 2017) *New York Times* http://www.nytimes.com/ (Accessed 09 August 2020).

T Shapshak “Note to Transnet: Cyberattacks Only Work When there are Vulnerabilities to Exploit” (4 August 2021) *Daily Maverik* https://www.dailymaverick.co.za/opinionista/2021-08-04-transnet-ports-closed-and-were-in-the-dark/ (Accessed 28 September 2021).

T-CY Cloud Evidence Group Crime Convention Committee “Criminal Justice Access to Data in the Cloud: Challenges (26 May 2015) *Discussion Paper Strasbourg;France* https://rm.coe.int/1680304b59 (Accessed 23 February 2022).

Techdirt “Stop saying ‘if you’re not paying, you’re the product’’ https://www.techdirt.com/articles/20121219/18272921446/stop-saying-if-youre-not-paying-youre-products.shtml (Accessed 25 February 2022).

Techopedia “Techopedia Explains Community Cloud” (2 May 2020) *Techopedia* http://www.techopedia.com (Accessed 13 July 2020).

The USA Patriot Act 2006: Preserving Life and Liberty, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (2003) *Department of Justice* https://www.justice.gov/ (Accessed 21 January 2021).

The Foreign Intelligence Surveillance Act of 1978: Justice Information Sharing U.S. Department of Justice: *Office of Justice Programs Bureau of Justice Assistance* https://it.ojp.gov/ (Accessed 21 January 2021).

U Yerrum “Data Security in the Cloud” (2012) *CSO* http://www.vormetric.com/sites/default/files/wp-data-security-in-the-cloud (Accessed 4 May 2020).

UEJF v Yahoo! Inc “TGI Paris Ordonnancede R6f6 Nos 00/05308, 00/05309 TGI Paris” (22 May 2000) *UEJF et Licra c/ Yahoo! Inc. et Yahoo France* http://juriscom.net (Accessed 10 July 2020).

V Reding “Privacy Matters: Why the EU Needs New Personal Data Protection Rules” (30 November 2010) http://europa.eu/rapid/pressReleasesAction (Accessed 20 July 2020).

Wikipedia https://en.wikipedia.org/wiki/Phishing (Accessed 21 February 2022).

Yahoo! inc v La Ligue Contre le Racisme et l'Antisemitisme et al, 169 F. Supp. 2d 1181 (N.D. Cal.2001) http://law.justia.com/cases/federal/district-courts/FSupp2/169/1181/2423974/ (Accessed 10 July 2020).