the global voice of the legal profession

IBA Intellectual Property, Communications and Technology Law Committee

Digital Regulations in the Metaverse Era

SOUTH AFRICA

Regional coordinator:
Docia Agyemang Boakye *technology and innovation lawyer, Accra*

Data

Regional coordinator – Docia Boakye Agyemang *technology and innovation lawyer, Accra*
Professor Sylvia Papadopoulos *University of Pretoria, Pretoria*

Q 1. Are there any data (personal and non-personal) policies, strategies or regulations applicable to the metaverse in your jurisdiction?

Yes. In addition to the right to privacy as contained in common law and section 14 of the Constitution of the Republic of South Africa of 1996, the South African regulatory framework includes some legislation that relates, either directly or indirectly, to various aspects of the right to privacy, data processing, information collection and retention. The applicable laws are:

- the National Credit Act 34 of 2005 (the NCA), which provides safeguards for personal information collected while concluding credit agreements that fall within the act's scope of application;[1]
- the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) prohibits the interception of both direct and indirect communications without a court order.[2] For our purposes, 'indirect communication' means the transfer of information, including a message or any part of a message, whether in the form of speech, music or other sounds, data, text, visual images, signals or radio frequency spectrums.[3] However, significant parts of RICA were declared unconstitutional in the *AmaBhungane Centre for Investigative Journalism* case;[4]
- the Promotion of Access to Information Act 2 of 2000 (PAIA) provides data protection insofar as it governs access to personal information and prohibits access to that information if such access would lead to an unreasonable violation of a person's privacy.[5] The PAIA allows access to 'records'[6] containing personal information (as defined by the Protection of Personal Information Act 4 of 2013 (POPIA)) in either hardcopy or digital format.[7] Section 3 of this act specifies that it is applicable to records held by both public and private bodies, without regard to when the record was created.[8] In all requests for access to information, access is contingent on the applicant fulfilling all the procedural requirements outlined in the act;[9] and
- POPIA is the most important data protection legislation in South Africa.

1 According to s 4, the NCA applies to every credit agreement between parties dealing at arm's length and made within, or having an effect within, the Republic of South Africa. For exceptions see ss 4(a)–(d) NCA.
2 See s 2 of RICA.
3 See s 1 of RICA.
4 *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others 2021* (3) SA 246 (CC).
5 See ss 33 and 64 of PAIA.
6 In s 1 of PAIA a 'record' is defined as '…of, or in relation to, a public or private body, means any recorded information- (a) regardless of form or medium; (b) in the possession or under the control of that public or private body, respectively; and (c) whether or not it was created by that public or private body, respectively'.
7 See ss 4-8 of PAIA.
8 See the definitions for public and private bodies below. In s 11 of PAIA, a right of access to the records of public bodies is provided, while s 50 provides for a right of access to the records of private bodies.
9 See ss 17–32 of PAIA, which provide for the manner of access to information from public bodies, and ss 53–61, which provide for the manner of access to information from private bodies, including forms and fees.

2. How is the various personal and non-personal data associated with the metaverse protected in your jurisdiction?

The application of POPIA starts with section 3, which states that POPIA:[10]

> '…applies to the processing of personal information (a) entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and (b) where the responsible party is (i) domiciled in the Republic; (ii) or not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are only used to forward personal information through the Republic.'

Two of the most important definitions for the application of POPIA include the definitions of 'personal information' and 'processing'. Personal information is defined as:

> 'Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to information relating to:
>
> a) the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
>
> b) the education or the medical, financial, criminal or employment history of the person;
>
> c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
>
> d) the biometric information of the person;
>
> e) the personal opinions, views or preferences of the person;
>
> f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
>
> g) the views or opinions of another individual about the person; and
>
> h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person'.

The list of information that is included in the definition is not exhaustive.[11] POPIA is unique because it also protects the personal data of a juristic person, where applicable.

Processing is so widely defined that it clearly intends to cover any action that could possibly be executed in respect of personal information, from initial collection to the dissemination or storage and eventual destruction of data.[12] This includes:

> '[A]ny operation or activity or any set of operations, whether by automatic means or not, concerning personal information, including (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information'.[13]

However, section 6(1) of POPIA exempts processing personal information for personal/household activities, de-identified data, national security tasks, criminal investigation/prosecution and court judicial functions, provided there are adequate legislative safeguards in place.

10 There are key terms or phrases in s 3 of POPIA that are important for precisely delineating the act's scope of application, such as 'processing', 'personal information', 'record', 'responsible party', 'filing system' and 'automated means'.

11 Yvonne Burns and Ahmore Burger-Smidt, *Protection of Personal Information: Law and Practice* (2nd edn, Lexis Nexis 2023) 58.

12 Sylvia Papadopoulos and Sizwe Snail ka Mtuze, *Cyberlaw@SA: The Law of the Internet in South Africa* (4th edn, Van Schaiks 2022) 352.

13 See s 1 of POPIA.

Section 7 of POPIA excludes the processing of personal information for journalistic, literary or artistic purposes if it balances privacy rights with freedom of expression in the public interest.[14]

Sections 37 and 38 of POPIA provide exemptions allowing the regulator to authorise the processing of personal information that may contravene the act if it is substantially in the public interest or clearly benefits the data subject, as notified in the South Africa's *Official Gazette of Record*.[15]

Q 3. Who are the different stakeholders involved in the data value chain in the metaverse and, in the case of personal data, what are their data protection roles? How are their activities regulated under regional/national policies, strategies or regulations?

Stakeholders

Responsible party and operator

As the central figure responsible for ensuring compliance with POPIA, the 'responsible party' is any private or public body or any other person, which alone or in conjunction with others, determines the purpose of and means for processing personal information.[16] This is true even if the processing is delegated to a service provider or other third party, referred to as an 'operator' in the act.[17] The 'operator' is a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that responsible party.[18]

Section 1 defines a 'public body' as any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government, or any other functionary or institution when exercising a power or performing a duty in terms of the constitution or a provincial constitution, or exercising a public power or performing a public function in terms of any legislation. A 'private body' refers to a natural person who carries or has carried on any trade, business or profession, but only in such capacity; a partnership that carries or has carried on any trade, business or profession; any former or existing juristic person; or a political party; but excludes a public body.

The Information Regulator (IR)

Section 39 of POPIA establishes the IR of South Africa and chapter 5 of POPIA sets out the jurisdiction, powers, duties, functioning, appointment, term of office and removal of members of the regulator, remuneration, allowances, benefits, and privileges of members of the IR and its office (sections 39–56 of POPIA).

Regulation

Jurisdiction and nature of the IR

The IR has jurisdiction throughout South Africa. It operates independently, subject only to the constitution and the law, and must remain impartial. It must carry out its functions in accordance with POPIA and PAIA. The regulator is accountable to the National Assembly.[19]

Powers, duties and functions of the IR[20]

The IR's role includes educating the public about the lawful processing of personal information; monitoring and enforcing compliance with POPIA by both public and private bodies; consulting and engaging with stakeholders on matters affecting personal information; handling complaints regarding the violation of personal information protections; conducting research and reporting to Parliament on international instruments and legislative amendments related to personal information protection; issuing, amending or revoking codes of conduct and assisting in their application;

14 See s 7(2) of POPIA.
15 See s 37(1)(a)-(b) of POPIA.
16 See s 1 of POPIA.
17 *Ibid*.
18 *Ibid*.
19 See s 39 of POPIA.
20 See s 40(a)–(h) of POPIA.

facilitating international cooperation on privacy-related law enforcement; performing any other functions necessary or incidental to its main functions; and exercising additional powers and duties conferred by POPIA and other legislation.[21]

Q 4. In relation to personal data, what are the data protection principles (eg, transparency) applicable in the metaverse?

In terms of section 4 of POPIA, there are eight conditions for the lawful processing of personal information. These are:

- **condition 1:** accountability (section 8);
- **condition 2:** processing limitation (sections 9–12);
- **condition 3:** purpose specification (sections 13 and 14);
- **condition 4:** further processing limitation (section 15);
- **condition 5:** information quality (section 16);
- **condition 6:** openness (sections 17 and 18);
- **condition 7:** security safeguards (sections 19–22); and
- **condition 8:** data subject participation (sections 23–25).

A legal justification should exist for the processing to be lawful and reasonable in terms of section 11, including consent, the performance of a contract, legal obligations, the protection of interests, public duty performance, or the pursuit of legitimate interests by the responsible party or a third party. Consent in POPIA is defined as any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.[22]

The security of personal information is a paramount concern for most data subjects and, as such, condition 7 is that of 'security safeguards' contained in sections 19–22. 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 the loss or damage to or unauthorised destruction or unlawful access to, or processing of personal information.[23]

In terms of sections 20 and 21 of POPIA, the application of security measures also extends to any operator or anyone processing personal information on behalf of a responsible party or on behalf of an operator. In the event of a security breach, as envisaged by section 22, the responsible party has a legal duty to report the breach to the data subject, as well as to the IR.[24]

Condition 8 gives data subjects two core rights, namely the right to access their personal information and the right to the correction or deletion of their personal information.[25]

Q 5. What are the most common types of infringement of data protection principles in the metaverse (eg, data minimisation) in your jurisdiction?

The most common types of infringements in the metaverse are most likely to be related to inadequate data minimisation, unclear jurisdictional applications, insufficient consent mechanisms and non-compliance with cross-border data transfer requirements.

In South Africa, as in other parts of the world, the metaverse poses a variety of data protection challenges. One key issue is the management of massive amounts of personal data collected as users navigate different virtual spaces

21 See s 40(a)–(h) POPIA
22 See s 1 POPIA.
23 See s 19(1) POPIA.
24 See s 22(1) POPIA.
25 See ss 23-25 POPIA.

within the metaverse. The difficulty lies in establishing contractual accountability and privacy obligations to protect this data, especially when it involves cross-border data transfers, which are common in the metaverse's globally connected environment.[26]

Another challenge is determining jurisdiction in regard to data protection laws in the metaverse. Since the metaverse connects a user to its avatar, creating a digital representation that can collect personal data, existing privacy and data protection laws are likely to apply. However, the application of these laws is complex due to the variety of possible jurisdictions that may be applicable, including the user's location, the avatar's location or the server's location. The tangled web of relationships within the metaverse could make it difficult to assign clear roles for responsible parties and operators.[27]

Regarding the different types of infringement, the metaverse's ability to observe users continuously can lead to more sophisticated ways of monitoring behaviour, and this deep level of behavioural analysis brings about the need for strict compliance with data protection laws, especially concerning the processing of sensitive data, such as biometric information gathered through virtual reality (VR) headsets or children's data.[28]

Q 6. What sanctions (civil, criminal or administrative) may apply?

Sanctions under POPIA

Civil actions

Section 99 of POPIA allows for civil actions against responsible parties for data protection violations, including breaches of information protection principles, non-compliance with specified sections or breaches of conduct codes, providing a strong incentive for compliance.[29] This section is significant in that the data subject does not need to prove that the responsible party was negligent or that it was acting intentionally, meaning that the responsible part is held strictly liable for damages.[30]

The defences that may be raised by a responsible party against a civil action for damages include *vis maior*, consent by the plaintiff, a fault of the plaintiff, that compliance was not reasonably practicable in the circumstances, or that the regulator authorised the breach in terms of section 37.[31]

Criminal offences and penalties

The following constitute criminal offences for which the sanctions include fines and/or imprisonment:

- hindering, obstructing or unlawfully influencing the regulator;[32]
- a breach of confidentiality, that is, any person who contravenes the provisions of section 54;[33]
- the failure to comply with an enforcement or information notice;[34]
- offences by witnesses;[35]
- an unlawful act by a responsible party with an account number;[36] and
- an unlawful act by a third party with an account number.[37]

26 Norton Rose Fulbright, 'The Metaverse: The evolution of a universal digital platform' (November 2022) www.nortonrosefulbright.com/en/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform accessed 4 April 2024.
27 *Ibid*.
28 *Ibid.*
29 See s 99 read with s 73 of POPIA.
30 See s 99(1) of POPIA.
31 See s 99(2) of POPIA.
32 See s 100 of POPIA.
33 See s 101 of POPIA.
34 See s 103 of POPIA.
35 See s 104 of POPIA.
36 See s 105 of POPIA.
37 See s 106 of POPIA.

The more serious of these offences draw a fine or imprisonment for a period not exceeding ten years, or both a fine and imprisonment. If convicted of the less serious offences in sections 59, 101, 102, 103(2) or 104(1), the sanctions include a fine or imprisonment for a period not exceeding 12 months, or both a fine and imprisonment.[38]

If a responsible party is alleged to have committed an offence in terms of this act, the regulator may ensure that an 'infringement notice' be delivered by hand to the offender.[39] With this notice, it is possible for the offender to pay an administrative fine up to ZAR 10m or elect to be tried in court on a charge of having committed the alleged offence referred to in terms of the act.[40] If an infringer elects to be tried in court on a charge of having committed the alleged offence in terms of the act, the regulator must hand the matter over to the South African Police Service and inform the infringer, accordingly.[41]

Q 7. Is there any case law or are there any decisions by a regulator regarding infringements of data protection principles in your region/country?

The courts have not had the opportunity to engage with POPIA yet and, therefore, there is no judicial precedent to mention.

However, the IR has issued enforcement notices to the South African Police Services in 2020; the Department of Justice and Constitutional Development in South Africa in 2021; Dis-Chem Pharmacy Group for a security breach at a third-party service provider (operator) in 2023; and against a direct marketing company in 2024, namely FT Rams Consulting, for continuing to send spam (direct marketing) despite multiple requests by a data subject to opt out of receiving the emails.

On 3 July 2023, the IR issued its first administrative fine of ZAR 5m against the Department of Justice and Constitutional Development for its failure to comply with an enforcement notice issued by the regulator under POPIA. The Department of Justice and Constitutional Development did not exercise its right to appeal the enforcement notice, nor did it comply with it.

Q 8. In relation to non-personal data, how is data sharing/licensing regulated in your jurisdiction?

The regulation of data sharing and licensing in South Africa, especially concerning non-personal data, is not explicitly outlined. Current legislation, such as POPIA, focuses mainly on personal data. For non-personal data, there isn't a clear regulatory framework detailed in the provided sources. However, South Africa has been active in aligning the country with global best practices on data protection and privacy as it applies to personal data, with the expectation that more comprehensive data laws, possibly extending to non-personal data, will follow.

Q 9. Is data ownership recognised in your jurisdiction?

Despite South Africa's recent policy, legislative and regulatory responses to a data intensive and driven economy,[42] there is no policy to guide localised data acquisition, ownership, storage, use and analytics. The government recognises this as a threat to both national security and social and economic growth.[43] A report by the Presidential Commission on the Fourth Industrial Revolution recommends that South Africa '[S]ecures and avails data to enable innovation'.[44]

38 See s 107 of POPIA.
39 See s 109(1) and (2) of POPIA. An infringement notice must contain certain minimum information.
40 See s 109(3) of POPIA.
41 See s 109(4) of POPIA.
42 Eg, the South African Government's *White Paper on Science Technology and Innovation* (2019) www.dst.gov.za/images/2019/White_paper_web_copyv1.pdf and the *National Integrated ICT Policy White Paper* (2016) www.gov.za/sites/default/files/gcis document/201610/40325gon1212.pdf and *the National e-Government Strategy and Roadmap* (2017) www.gov.za/sites/default/files/gcis_document/201711/41241gen886.pdf accessed 5 June 2024.
43 Draft National Data and Cloud Policy (2021) as published in *Official Gazette of Record* No 44389 on 1 April 2021 www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf accessed 4 April 2024.
44 Recommendation 4 of the Report of the Presidential Commission on the 4th Industrial Revolution (2020) 51 www.dcdt.

The South African Draft National Data and Cloud Policy would seem to suggest that data generated in South Africa could be considered the property of South Africa, regardless of where the technology company is domiciled. This policy framework aims to align with the POPIA, and suggests that the Department of Trade, Industry and Competition, through entities like the Companies and Intellectual Property Commission (CIPC), will develop a policy framework for the data generated in such contexts, including the sharing and use of such data.[45]

It is crucial to note that while the concept of data ownership is being discussed, it does not translate to a clear, unequivocal legal principle that is currently enforceable. Although interestingly, the Cybercrimes Act 19 of 2020 contains section 12, which states that the common law offence of theft must be interpreted so as not to exclude the theft of incorporeal property.

Q 10. How is proprietary information, including any rights to datasets, regulated in your jurisdiction?

In South Africa, proprietary information, including rights to personal data datasets, is regulated primarily under POPIA, which came into effect on 1 July 2020. POPIA applies to the processing of personal information entered into a record by a responsible party using automated or non-automated means, provided the responsible party is domiciled within South Africa or uses means within South Africa for such processing.[46] The act defines 'automated means' as equipment capable of operating automatically in response to instructions for the purpose of processing information.[47]

Businesses are required to register their information officers,[48] and while there's generally no obligation to notify the IR of every data processing activity, prior authorisation may be needed for certain processing activities, especially those involving special personal information or the personal information of children.[49] Section 57 of POPIA outlines conditions under which a responsible party must seek prior authorisation from the IR before processing certain types of data. This section includes the following activities that require prior authorisation:

- unique identifiers: if processing unique identifiers of data subjects for a different purpose than originally intended or to link data with information processed by others;
- criminal behaviour: if processing data on criminal behaviour or unlawful or objectionable conduct on behalf of third parties;
- credit reporting: if processing personal information for credit reporting purposes; and
- the transfer of special personal information: if transferring special personal information or that of children to a foreign country that does not have adequate data protection measures in place.

Additionally, this section provides the regulator with the authority to apply these requirements to other processing activities that may pose risks to the interests of data subjects.[50] Lastly, it states that these requirements do not apply if there's a relevant code of conduct in effect within a specific sector.[51]

Q 11. What are the most common types of infringement of these rules in the metaverse (eg, unlawful use of proprietary information) in your jurisdiction?

N/A.

gov.za/documents/reports/file/241-report-of-the-presidential-commission-on-the-4th-industrial-revolution-south-african-government-www-gov-za.html accessed 4 April 2024.

45 Draft National Data and Cloud Policy (2021) as published in Official Gazette of Record No 44389 on 1 April 2021 www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf accessed 4 April 2024.

46 See s 3 of POPIA.

47 See s 3(4) of POPIA.

48 See ss 55 and 56 of POPIA.

49 See s 57 of POPIA

50 See s 57(2) of POPIA.

51 See ss 60-68 of POPIA.

12. Are there any policies, strategies or regulations applicable to digital marketing in the metaverse in your jurisdiction?

Activities that fall under the broad banner of 'direct marketing' are regulated by both the Consumer Protection Act 68 of 2008 (the 'CPA') and POPIA.

The CPA

Part B of chapter 2 of the CPA contains the consumer's right to privacy but regulates aspects of direct marketing and places limitations on suppliers who are engaged in direct marketing. Section 11 sets down that a consumer has the right to refuse to accept, require another person to discontinue or pre-emptively block any approach or communication if the approach or communication is primarily for direct marketing purposes.[52] To facilitate this, the National Consumer Commission (NCC) is required to establish a registry, where a person may register a pre-emptive block against direct marketing communications and any person authorising, directing or conducting any direct marketing must implement appropriate procedures to facilitate demands to stop further communications (as of March 2024, no registry has been established).[53]

Furthermore, section 12 read with the CPA regulations determines the times that the supplier may contact a consumer for direct marketing purposes.

POPIA

Chapter 8 of POPIA designates 'the rights of data subjects regarding direct marketing via unsolicited electronic communications, directories and automated decision making'. In turn, direct marketing means an approach to a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of (a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or (b) requesting the data subject to make a donation of any kind for any reason.[54] Direct marketing has the same provisos as the CPA's definition, suffice to say that the term 'person', is used in the CPA and 'data subject' in POPIA. A data subject can be either a natural person or a legal person and, therefore, both business-to-consumer (B2C) and business-to-business (B2B) marketing are included.[55]

Section 69(1) of POPIA prohibits the processing of personal information of a data subject for the purpose of direct marketing through any form of electronic communication, including automatic calling machines,[56] facsimile machines, SMSs or emails (the last three terms are not defined in POPIA).[57] Thus, the key term here is 'electronic communication' because if the direct marketing does not take place through a medium of electronic communication then the stringent provisions of section 69 of POPIA do not apply to the direct marketer.[58] This does not mean the rest of POPIA's provisions do not apply. The direct marketers still have to comply with the requirements of lawful processing (sections 8–25) and other provisions in the act, as well as relevant provisions of the CPA.

Nevertheless, electronic communications include any text, voice, sound or image message sent over an electronic communications network, which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.[59] De Stadler et al interpret this definition of electronic communication as including the listed forms of communication, that is automatic calling devices (robocalls), faxes, emails and SMSs, and so-called push notifications or in-app direct messages. They are also of the opinion that telephone calls (whether transmitted through mobile networks, fixed networks or voice over internet protocols (VOIP)), standard physical postage, targeted social media marketing or behavioural advertising are not electronic communications, as defined in POPIA.[60]

52 See s 11(1) and (2) of CPA.
53 See s 11(3) of CPA, Sylvia Papadopoulos in Evert Van Eeden and Jacolien Barnard, *Consumer Protection Law in South Africa* (2nd edn, LexisNexis Durban 2017) 588.
54 See s 1 of POPIA.
55 Elizabeth De Stadler; Ilze Luttig Hattingh; Paul Esselaar and Jessica Boast, *Overthinking the Protection of Personal Information Act* (Juta 2022) 471.
56 See s 69(5) of POPIA, which defines an 'automatic calling machine' as 'a machine that is able to do automated calls without human intervention'.
57 Sylvia Papadopoulos and Dire Tladi in n 11 above 133.
58 See n 55 above 475.
59 See s 1 of POPIA.
60 See n 55 above 476–479.

However, section 69(1) of POPIA does attempt to broaden the scope by indicating that the processing of personal information of a data subject for the purpose of direct marketing through any form of electronic communication is prohibited unless the data subject has given consent. Burger-Smidt argues that the use of the word 'including' in section 69(1) means that the forms of electronic communication listed in the section 1 definition are not a *numerus clausus* (not a finite list) and that it could include other forms of electronic communication.[61]

The IR has recently taken the view that telemarketing falls within the definition of electronic communication by issuing an enforcement notice to FT Rams Consulting on 27 February 2024 and, therefore, it is direct marketing that is regulated under section 69 of POPIA.

Previously, the author has noted with disappointment that section 69(2) was included in POPIA. This section allows a responsible party to approach a data subject once, to request consent for the sending of direct marketing material if consent has not previously been withheld.[62]

This section is strongly opposed due to its scope for abuse and because it reverts to an opt-out model. In fact, by allowing a responsible party to process personal information to make the approach 'once' to get consent, the prohibition in section 69(1) is reduced to a second-level protection mechanism, that is, it only becomes relevant after the approach for consent has been made.[63] The 'contact once' provision also potentially undermines the position established in the CPA, where a direct marketer must, without exception, assume that a consumer has registered a comprehensive pre-emptive block.[64] The practical implementation of this would require marketers to enquire at the registry whether a block has been registered. If a block has been registered by the consumer, the marketer will not be allowed to exercise the 'contact once' option in section 69(2). The problem is that the registry has not been established and therefore this layer of protection is non-existent.[65]

Throughout POPIA, consent must be a voluntary, specific and informed expression of will.[66] Section 69(2)(b) sets additional criteria for consent in the direct marketing context, that is the data subject's consent must be requested in the prescribed form and manner.

The discussion above relates to direct marketing sent to a data subject where there is no prior nexus. Nevertheless, where there is a nexus, in terms of section 69(3) of POPIA, a responsible party may process the personal information of a data subject who is a customer of the responsible party for direct marketing purposes, if the responsible party:

- has obtained the contact details of the data subject in the context of the sale of a product or service;
- it is for the purpose of direct marketing of the responsible party's own similar products or services; and
- if the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of its electronic details either:

  at the time when the information was collected; or on the occasion of each communication with the data subject for the purpose of marketing, if the data subject has not initially refused such use.

Thus, all three requirements need to be met in terms of section 69(3)(a)–(c). The key question here is, when will the data subject be a customer of the responsible party? A customer is not defined in POPIA. It is also not yet certain whether there would have to be a completed commercial transaction for goods or services between the data subject and the responsible party before the data subject is a customer or if mere browsing on a website as a potential customer or an enquiry (either in the form of a search engine search or actual online communication with the responsible party) is sufficient.

61 See n 11 above, 528.

62 Sylvia Papadopoulos, 'Are We About to Cure the Scourge of Spam? A Commentary on Current and Proposed South African Legislative Intervention' 2012 THRHR 223–240; and Bernard Hamann and Sylvia Papadopoulos, 'Direct Marketing and Spam Via Electronic Communications: An Analysis of The Regulatory Framework in South Africa' (2014) *De Jure* 42. See s 69(2)(b) of POPIA, the consent will have to in a prescribed form and manner.

63 Lee Swales, 'Protection of Personal Information: South Africa's Answer to the Global Phenomenon in the Context of Unsolicited Electronic Messages (Spam)' (2016) SA Merc LJ 49; Bernard Hamann and Sylvia Papadopoulos, 'Direct Marketing and Spam Via Electronic Communications: An Analysis of The Regulatory Framework in South Africa' (2014) De Jure 42. See n 55 above 488–490, where the authors point out one of these abuses, which is if a responsible party's products or services, or the method of communication for the direct marketing changes after the data subject was first approached for consent under s 69(2) of POPIA, they can approach the data subject for a second or third time to obtain consent for the new direct marketing purpose.

64 CPA Reg 4(3)(g).

65 See n 57 above, 131.

66 See s 1 of POPIA for the definition of 'consent'.

What may be indicative and in line with a purposive interpretation is that section 69(3) require a responsible party to obtain the contact details of the data subject in the 'context of the sale of a product or service'. When the contact details would be shared within the context of the sale of a product or service is likewise open to interpretation and will be determined on the facts at hand. What can be stated is that 'sale' is a very specific type of transaction in South African law and that the contact details obtained in the context of, for example, a contract of lease would not entitle the lessor/responsible party to engage in direct marketing to the lessee/data subject.[67]

Direct marketing by the responsible party to the customer is also limited to similar products or services that were the subject of the sale that created the nexus between the data subject and the responsible party. This means that section 69(3) cannot be used to cross-sell different products or services.[68] Section 69(4) of POPIA requires any communication for direct marketing purposes to contain details on the identity of the sender or the person on whose behalf the communication has been sent and an address or other contact details to which the recipient may send a request that such communications cease (request to unsubscribe).

The data subject must be given the ability to unsubscribe or request that direct marketing cease under section 69(3)(c) and to object to the processing of personal information pursuant to section 11(3)(b) of POPIA. Section 69(3)(c) concerns situations where the responsible party is marketing to its customers and the opportunity to unsubscribe must be given free of charge and without unnecessary formality at the time of the collection of personal information and in each subsequent communication. While section 11(3)(b) states that the data subject can also object at any time to the processing of personal information for direct marketing purposes that is not in the form of an unsolicited electronic communication as referred to in section 69. Thus, differentiation between direct marketing via unsolicited electronic communications and all other direct marketing is made between section 69 and section 11 of POPIA.

A data subject who is included in a printed or electronic directory of subscribers that is available to the public or obtainable through directory enquiry services, in which their personal information is included, must be informed, free of charge and before the information is included in the directory, of the purpose of the directory and any further uses to which the directory may be subject.[69]

They must furthermore be given a reasonable opportunity to object to the use of the personal information or to request verification, confirmation or withdrawal of such information if the data subject has not initially refused such use.[70] A subscriber is any person who is party to a contract with the provider of a publicly available electronic communications service for the supply of such services.[71]

Q 13. What is the age of consent for data protection purposes?

In South Africa, a 'child' or a minor means a natural person under the age of 18 years old who is not yet legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning itself. A 'competent person' is defined as any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.[72]

67 Nagel et al (2016) 197 state that a contract of sale is a specific, nominate, reciprocal agreement to buy and sell, in terms of which the seller has a true intention to deliver a determined or determinable thing together with all their rights in the thing, undisturbed to the buyer and the buyer has the true intention of paying a determined or determinable price for the thing. Therefore, the *essentialia* that distinguish a contract of sale from all other contracts are: (a) the intention of the buyer to buy and the seller to sell, (b) that there is a thing (*merx*) which is bought and sold and (c) there is a purchase price.

68 Cf n 55 above, 495.

69 See s 70 of POPIA.

70 See s 70(2) of POPIA, but in terms of s 70(3), ss 70(1) and (2) do not apply to editions of directories that were produced in printed or offline electronic form prior to the commencement of this section and, in terms of s70(4), if the personal information of data subjects who are subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the information protection principles prior to the commencement of this section, the personal information of such subscribers may remain included in this public directory in its printed or electronic versions, after having received the information required by ss 70(1).

71 See s 70(5) of POPIA.

72 See s 1 of POPIA.

14. Is it necessary to verify the consent provided by a responsible adult?

No, verification is not explicitly required in South Africa.

15. How are international data transfers regulated in your jurisdiction?

When personal information is transferred from responsible parties or operators to other recipients in other countries or to international organisations, the level of protection given to data subjects under POPIA should not be undermined. However, in cross-border transfers of information, it is important to distinguish between simply routing electronic information through one country on its way to another (which is usually the case for email as it transitions across servers) and the actual transfer of personal information so that it can be processed in another country.

Section 72 of POPIA was specifically included in view of these requirements. It provides that a responsible party in the Republic of South Africa may not transfer personal information about a data subject to a third party who is in a foreign country unless the third-party recipient is subject to a law, binding corporate rules or a binding agreement that provides an adequate level of protection, which upholds principles for the reasonable processing of the information that are 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.

Under section 72(1), exceptions to the data transfer rules include: the data subject's consent; the transfer is a necessity for contracts or pre-contractual measures; the contract is in the data subject's interest; and transfers benefiting the data subject where consent cannot be reasonably obtained but are likely to be given.

16. Is there any case law or are there any decisions by a regulator regarding infringements of these rules in your jurisdiction?

There are no relevant cases or decisions in South Africa.

17. How is automated decision-making regulated in your jurisdiction?

On 'automated decision making', section 71 stipulates that no one may be subject to a decision that has legal consequences, or that affects them to a substantial degree, which is taken solely on the basis of the automated processing of personal information intended to create a profile on certain aspects of their personality or personal habits, such as performance at work, credit worthiness, reliability, location, health, personal preferences or conduct.

Section 71(1) of POPIA does not apply to automated decision-making in contractual contexts if the data subject's request is met, their interests are protected or such decision-making adheres to a law or code with specified protections, including rights to representation and information on the logic of processing.[73]

73 See s 71(3) of POPIA.

18. What rights are granted to individuals for protecting their rights in the metaverse and how can they be exercised?

Protecting rights

PAIA

The enforcement of the PAIA also falls to the IR, established under sections 39–54 of POPIA.[74] Most importantly, deliberately obstructing access to records under PAIA by destroying, damaging, altering, concealing, falsifying or creating a false record is a criminal offence. Anyone found guilty of such actions could face imprisonment for up to two years or a fine on conviction.[75]

POPIA

Under POPIA, a complaint about personal information interference pertains to a breach of lawful data processing, ignoring specified sections or violating a code of conduct. Complaints must be made in writing.[76]

On receiving a complaint in terms of section 74, the regulator must investigate and conduct a full investigation into the complaint, or they can decide to take no action in response to the complaint (sections 76 and 77), or refer the complaint to the enforcement committee.[77] The regulator may also, of its own accord, commence an investigation into an interference with the protection of the personal information of a data subject (section 73).

If it appears that it may be possible to secure both a settlement between any of the parties concerned and an appropriate assurance against the repetition of any action that resulted in the complaint, the regulator may, without investigating the complaint, use its best endeavours to secure a settlement.[78]

In the enforcement of POPIA, the regulator has the power to summon and enforce the appearance of persons and compel them to give evidence under oath and to produce any records needed.[79] The regulator may obtain warrants to enter and search premises.[80] Under section 90(1), the regulator may serve a responsible party with an 'information notice', requiring the party to provide an independent report in respect of the information processing activities or information relating to compliance with the act.[81]

After completing the investigation into a complaint or other matter in terms of this act, the regulator may refer the complaint or other matters to the enforcement committee for consideration.[82]

19. What is the level of enforcement based on private claims in your jurisdiction?

Under PAIA, there is a high level of enforcement through private litigation, but this is not so in terms of POPIA, as yet.

20. Are there any upcoming policies, strategies or regulations that will impact the use of data in the metaverse?

None are noted at this stage.

74 The schedule to POPIA read with s 110, see n 11 above 585.
75 See s 90 of PAIA.
76 See ss 73–75 of POPIA.
77 See s 76(1)(a)–(f) of POPIA.
78 See s 80 of POPIA.
79 See s 81 of POPIA.
80 See ss 82–88 of POPIA.
81 See s 90(2) of POPIA.
82 See s 92 of POPIA.

Bibliography

Legislation

The Constitution of the Republic of South Africa of 1996.

The National Credit Act 34 of 2005 (the NCA).

The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA).

The Promotion of Access to Information Act 2 of 2000 (PAIA).

The Protection of Personal Information Act 4 of 2013 (POPIA).

The Consumer Protection Act 68 of 2008 (the 'CPA').

The Consumer Protection Act Regulation No R 293 of 1 April 2011, published in the *Government Gazette* No 34180.

The Determination of Threshold in Terms of the Consumer Protection Act 68 of 2008 Regulation No R 294 of 1 April 2011, published in *Government Gazette* No 34181.

Cases

AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others 2021 (3) SA 246 (CC).

Books

- Evert Van Eeden and Jacolien Barnard, *Consumer Protection Law in South Africa* (2nd edn, LexisNexis Durban 2017).
- Elizabeth De Stadler, Ilze Luttig Hattingh, Paul Esselaar and Jessica Boast, *Overthinking the Protection of Personal Information Act* (Juta 2022).
- Sylvia Papadopoulos and Sizwe Snail Ka Mtuze, *Cyberlaw@SA: The Law of the Internet in South Africa* (4th edn, Van Schaiks 2022).
- Yvonne Burns and Ahmore Burger-Smidt, *Protection of Personal Information: Law and Practice* (2nd edn, Lexis Nexis 2023).
- CJ Nagel and B Prozesky-Kushke (eds), J Barnard, A Boraine, M Botha, R Brits, H Coetzee, EP Joubert, KM Kern, DJ Lötz, K Newaj, JM Otto, S Papadopoulos, S Renke, M Roestoff and BPS Van Eck, *Commercial Law* (7th edn, LexisNexis: South Africa 2019).

Websites

See the published enforcement notice and media statement https://inforegulator.org.za/wp-content/uploads/2020/07/MEDIA-STATEMENT-ENFORCEMENT-NOTICE-ON-DIRECT-MARKETING-COMPLAINT.pdf, accessed 11 March 2024.

Simnikiwe Mzekandaba, 'Direct Marketers Body Studies InfoReg's Latest Classification' (1 March 2024) ITWeb www.itweb.co.za/article/direct-marketers-body-studies-inforegs-latest-classification/wbrpOMg2pdX7DLZn, accessed 10 March 2024.

Articles

- Bernard Hamann and Sylvia Papadopoulos, 'Direct Marketing and Spam Via Electronic Communications: An Analysis of The Regulatory Framework in South Africa' (2014) *De Jure* 42.
- Sylvia Papadopoulos, 'Are We About to Cure the Scourge of Spam? A Commentary on Current and Proposed South African Legislative Intervention' (2012) *Tydskrif vir Hedendaagse Romeins-Hollands Reg/ Journal for Contemporary Roman-Dutch Law* 223.
- Lee Swales, 'Protection of Personal Information: South Africa's Answer to the Global Phenomenon in the Context of Unsolicited Electronic Messages (Spam)' (2016) *South African Mercantile Law Journal* 49.

Cybersecurity

1. Are there any cybersecurity policies, strategies or regulations applicable to the metaverse in your jurisdiction?

Cybercrime and cybersecurity are two interconnected but distinct concepts. Cybercrime involves illegal activities, while cybersecurity involves measures to protect against such activities. They are interconnected, with cybersecurity efforts aimed at preventing and mitigating cybercrime.[83]

The National Cybersecurity Policy Framework (NCPF) was approved by Parliament in 2012, but it was only published in December 2015.[84] The purpose of the NCPF is to create a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of critical information infrastructure, while strengthening shared human values and the understanding of cybersecurity in support of national security imperatives and the economy.[85]

The NCPF defines cybersecurity as '…the practice of making the networks that constitute cyberspace secure against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them'.[86]

The laws considered relevant for cybersecurity in South Africa include:[87]

- the Constitution of the Republic of South Africa and in particular sections 14 on the right to privacy, section 32 on access to information and section 36 for limitations to rights contained in the constitution;
- the Promotion of Access to Information Act 2 of 2000 (PAIA) provides data protection insofar as it governs access to personal information and prohibits access to that information if the access would lead to an unreasonable violation of a person's privacy.[88] In all requests for access to information, access is contingent on the applicant fulfilling all the procedural requirements outlined in the act;[89]
- the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) prohibits the interception of both direct and indirect communications without a court order.[90] For our purposes, an 'indirect communication' means the transfer of information, including a message or any part of a message whether in the form of speech, music or other sounds, data, text, visual images, signals or radio frequency spectrums.[91] However, significant parts of RICA were declared unconstitutional in the *AmaBhungane Centre for Investigative Journalism* case;[92] and
- the Protection of Personal Information Act 4 of 2013 (POPIA) makes it obligatory for responsible parties and their operators to comply with specific conditions for the lawful processing of personal information.[93] The act also places an obligation on responsible parties to disclose breaches of information, provide data subjects with remedies and confers on the IR powers to impose penalties and other remedies for non-compliance or breach of the provisions of POPIA.[94]

Section 4 of POPIA sets out eight conditions for the lawful processing of personal information. These conditions are found in sections 8–25 of POPIA.[95] Of these conditions for compliance, the seventh condition places a duty on responsible

83 Watney in n 12 above, 464.
84 The National Cybersecurity Policy Framework (NCPF) (2015), 14 www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf, accessed 10 March 2024.
85 Para 3.1 of NCPF.
86 Para 1 'Definitions' NCPF (2015), 8.
87 Jason Jordaan and Sizwe Snail ka Mtuze in n 12 above, 499–504.
88 See ss 33 and 64 of PAIA.
89 See ss 17–32 of PAIA, which provide for the manner of access to information from public bodies, and ss 53–61, which provide for manner of access to information from private bodies including forms and fees.
90 See s 2 of RICA.
91 See s 1 of RICA.
92 See n 4 above.
93 See s 8 and s 20 of POPIA; see n 55 above, 3.
94 See s 22 and ss 100–109 of POPIA.
95 See discussion on conditions in n 12 above 348–367; see n 55 above; see n 11 above.

parties to apply appropriate and reasonable, technical and organisational steps to prevent the loss or damage to or unauthorised destruction of personal information, and unlawful access to or processing of personal information.[96]

In the event of a security breach, a responsible party must report it to IR and the data subjects affected.[97] Section 22 requires that such notification needs to be made within a reasonable period after discovery of the compromise, considering the needs of law enforcement.

The Critical Infrastructure Protection Act 8 of 2019 (the CIP Act) has as its purpose the identification of infrastructure as critical infrastructure, the establishment of the Critical Infrastructure Council and other functions aimed at preserving the country's critical infrastructure.[98] Within the context of information security, critical databases across various government departments, organisations and responsible actors hold information with a high level of importance, including the personal information of South Africans.[99] The qualifying criteria for what constitutes critical infrastructure is whether its functioning is essential for the economy, national security, public safety and the continuous provision of basic public services; and if the loss, damage, disruption or immobilisation of such infrastructure may severely prejudice the functioning or stability of the Republic of South Africa, the public interest with regard to safety and the maintenance of law and order and national security.[100] Chapter 5 sets out offences and penalties for contravention of the provisions of the CIP Act.

The Cybercrime Act 19 of 2021 is an important piece of legislation within the field of cybersecurity law. POPIA, although not strictly considered as an aspect of cybersecurity, but rather as a piece of legislation focused on data protection overlaps with the Cybercrime Act insofar as the latter relates to obligations surrounding the security safeguards to be put in place by private or public bodies processing personal information, or conversely to be respected and not compromised by other persons.[101]

In the public sector context, the Department of Public Service and Administration has gazetted various directives to guide government departments on information security in the absence of a national cybersecurity act. The key directives are outlined below.

The Directive on Public Service Information Security (2022) became applicable to all government departments from 7 June 2022.[102]

The directive requires departments to classify all information and incorporates the government's Minimum Information Security Standards of 1996 (MISS), within the definitions.[103] MISS first introduced the concept of classification, but MISS has four classifications and the directive only has three.[104] These are:[105]

1. public information: this information has been explicitly approved by management for release to the public;
2. confidential information: this information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. The unauthorised disclosure of this information could adversely impact the department or third parties; and
3. secret information: this is sensitive information that, if disclosed, has the ability to seriously and adversely impact a department or third parties.

The government departments must proactively manage four kinds of security occurrences: an incident, an information security event, an information security incident and a compromise. It also distinguishes between computer security and information security. Computer security would seem to be device security, while information security is about safeguarding information assets.[106]

96 See s 19 of POPIA.
97 See s 22(1) of POPIA.
98 Preamble to CIP Act and s 2 CIP Act.
99 See n 87 above, 505.
100 *Ibid*.
101 See n 83 above.
102 See www.dpsa.gov.za/dpsa2g/documents/ogcio/2022/egov_21_06_2022_directive.pdf, accessed 4 April 2024.
103 Pt 5 of the Directive on Public Service Information Security (2022).
104 Mbanjwa Michalsons 'Directive on Public Service Information Security | DPSA' (2022), www.michalsons.com/blog/directive-on-public-service-information-security-dpsa-2/59833, accessed 4 April 2024.
105 Pt 12 of the Directive on Public Service Information Security (2022).
106 See n 104 above.

As of 7 June 2022, departments are expected to develop and maintain an ongoing information security awareness programme to reduce human error.[107]

Departments must also use contracts to strengthen information security in two main ways:

1. all new government employees must sign a human resources (HR) policy that incorporates a summarised version of the mandatory information security policy and will form part of the employment contract; and
2. all contracts with software or system developers must include an intellectual property clause that prohibits developers from copying, selling, leasing or removing any software, information, source code or system design documents developed by or on behalf of a department.[108]

There are various duties assigned for:

- information system acquisition, development and maintenance;[109]
- physical security management[110] and HR security operations, including employee and user responsibilities;[111]
- under the heading 'Communications and Operations Management' there are rules on:[112]
  - system operations;
  - continuous vulnerability management;
  - protection against malicious and mobile code;
  - prohibited software, including bootleg software, illegal, pirated or reproduced copies of software or data;
  - powerful system tools or programs that are designed to investigate and/or exploit a department's information security environment (including password crackers, scanners, network sniffing devices, network packet sniffing devices and other hacking tools);
  - shareware/freeware or all software available from the internet, where no licensing requirements are given and personal/non-department software;
  - inappropriate content, images and/or text involving race, nudity or sexual themes are not appropriate for the workplace;
  - network security; and
  - protection of information security devices;
- password management;[113]
- mobile and remote computing;[114]
- outsourcing requirements;[115]
- cybersecurity,[116] where the head of department must ensure that penetration testing, vulnerability scans and threat risk analysis are part of the departmental cybersecurity initiatives;

107 Pt 11 of the Directive on Public Service Information Security (2022).
108 Pt 14 *ibid.*
109 Pt 13 *ibid.*
110 Pt 15 *ibid.*
111 Pt 16 *ibid.*
112 Pt 17 *ibid.*
113 Pt 21 *ibid.*
114 Pt 22 *ibid.*
115 Pt 24 *ibid.*
116 Pt 25 *ibid.*

- cloud security,[117] where the head of department must ensure that thorough due diligence of the service provider's integrity, legal agreements, physical location and security must be conducted before deciding on a cloud service provider;
- auditing and monitoring;[118] and
- information and communications technology (ICT) service continuity and disaster recovery.[119]

The second piece of legislation is the Directive on Cloud Computing in the Public Service (2022).[120] This legislation guides government departments on how to consider cybersecurity when adopting and using cloud services, and mentions that there will be a national cybersecurity act. The effective date of the directive was from 14 January 2022.

The Department of Public Service and Administration (DPSA) wrote this directive with the aim of encompassing all government departments and their personnel. It mandates adherence whenever government data storage or processing via cloud services is contemplated. This directive is also pertinent for cloud service providers as it enables them to discern the specific requirements of departments when tendering to provide cloud services.

The general requirements outlined in the directive include:

- departments must explore cloud services before considering on-premise alternatives;
- should they opt for cloud services, departments must ensure suitability and appropriateness tailored to their specific needs, ie, are they 'fit for purpose';
- the respective departmental head (HoD) must oversee adherence to proper procurement processes;
- departments must base their need for cloud services on operational requirements; and
- prior to the acquisition and deployment of cloud services, departments must furnish an approved business case and risk assessment to the DPSA.[121]

The pre-requisites before procuring cloud services are:

- departments must conduct a cloud readiness assessment before transitioning to cloud services;
- data classification must adhere to South Africa's national information security policy: (MISS). The classification type determines the permissible cloud model (public/hybrid/community/private) for departmental use;
- data must be kept within South Africa. If this isn't feasible, cloud service providers must comply with section 72 of POPIA;
- a department needs to conduct a risk assessment for each cloud service it intends to utilise;[122] and
- departments must formulate a business case that includes:[123]
  - the scope of the cloud services;
  - short, medium and long-term budget considerations;
  - the total cost of ownership over the medium and long term;
  - human resource requirements for supporting the cloud services;
  - the necessary infrastructure for facilitating cloud service operations (eg, broadband connectivity);
  - the intended departmental benefits from cloud service usage; and

117 Pt 26 *ibid.*
118 Pt 28 *ibid.*
119 Pt 29 *ibid.*
120 See www.dpsa.gov.za/dpsa2g/documents/egov/2022/egovernment_02_02_2022.pdf, accessed 4 April 2024.
121 Pt 9.2 of the Directive on Cloud Computing in the Public Service (2022). See also Nathan-Ross Adams Michalsons Attorneys 'Directive on Cloud Computing In The Public Service | DPSA' (2022), www.michalsons.com/blog/directive-on-cloud-computing-in-the-public-service-dpsa/55782, accessed 4 April 2024.
122 Pt 9.3 of the Directive on Cloud Computing in the Public Service (2022).
123 Pt 9.3.8 *ibid.*

- detailed outcomes of the risk assessment, a summary of the key risks and mitigation recommendations.

Importantly, the business case requires DPSA approval before cloud service usage, with periodic reviews thereafter.

Concerning the contractual obligations, at a minimum, contracts must stipulate:[124]

- the departmental ownership of the data;
- the service provider's responsibility for maintaining, backing up and securing data until returned to the department;
- the compliance with POPIA;
- the data storage and processing locations;
- the data storage and processing confined to locations, allowing adequate departmental control;
- the governing law and jurisdiction;
- provisions for data return or transfer in the event of provider takeover; and
- the disposition of data on contract termination.

During cloud service usage, the following is required:

- information security: departments must secure data in accordance with their information security policy;
- access rights: regular reviews of data access rights are imperative;
- scaling cloud services: scaling requires proper authorisation;
- asset inventory: departments must establish and maintain an inventory of data or applications;
- business continuity plans: post-implementation, departments must update and test their business continuity plans regularly; and
- backups: there must be backup mechanisms for departmental data, subject to regular review.[125]

Departments must ensure that the service provider transfers all departmental data and applications to the new provider, or per departmental discretion, return or destroy the said data or applications.[126]

Q 2. What are the security by design principles applicable to the metaverse in your jurisdiction?

N/A.

Q 3. Have there been any cyber incidents in the metaverse in your jurisdiction?

N/A.

124 Pt 9.3.11 *ibid.*
125 Pt 9.4 *ibid.*
126 Pt 9.5 *ibid.*

Q 4. How do the applicable policies, strategies or regulations react to cyber-incidents?

Regulation and sanctions under the Cybercrimes Act 19 of 2021

The Cybercrimes Act 19 was approved by the president on 1 June 2021 and came into operation on 1 December 2021. It repealed chapter 9 and sections 85, 86, 87, 88 and 90 of the ECT Act. However, crimes committed prior to the enactment of the Cybercrimes Act will still be prosecuted in accordance with the ECT Act and, therefore, knowledge of the relevant sections in the ECT Act will be of relevance for some time.[127]

The purpose of the act is to, among other things, create offences which have a bearing on cybercrime; to criminalise the disclosure of data messages that are harmful and to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the power to investigate cybercrimes; and to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrimes.[128]

Chapter 2 (sections 2–23) criminalises unwanted conduct and communication in cyberspace in line with international best practices.[129] The chapter is divided into six parts, as follows:

1. cybercrimes (part I);
2. malicious communications (part II);
3. attempting, conspiring, aiding, abetting, inducing, inciting, instructing, commanding or procuring to commit offence (part III);
4. competent verdicts (part IV);
5. sentencing (part V); and
6. orders to protect complainants from the harmful effect of malicious communications (part VI).[130]

Parts I and II provide for cybercrime and malicious communications, whereas parts III to VI may be considered miscellaneous aspects relevant to part I and part II. Parts I and II must be read with section 19 of the Act for the sentencing and penalty provisions.

It is also important to keep in mind the competent verdicts provided for in section 18, part IV. If the crime for which the accused is charged cannot be proven, then section 18 provides for the crime the accused may be convicted for.

According to Watney, part I may be broken down into broad categories of criminal offences.[131] This first category provides for offences against the integrity, confidentiality and availability of data, computer programs, data storage mediums and computer systems. This category criminalises cyber-dependent crimes that target data, computer programs, data storage mediums and computer systems.[132]

Section 2 of the act criminalises the unlawful and intentional access to a computer system or a computer data storage medium. Access to a computer data storage medium means that a person either uses data or a computer program stored on a computer data storage medium, or stores data or a computer program on a computer data storage medium. A person accesses a computer system if the person either uses data or a computer program held in a computer system or stores data or a computer program on a computer data storage medium that forms part of the computer system; or instructs, communicates with or otherwise uses the computer system. On conviction, section 19(1) provides for a fine or imprisonment for a period of five years, or both a fine and imprisonment.[133]

127 See n 83 above 475-476.
128 Preamble to the Cybercrime Act.
129 See n 83 above, 478.
130 *Ibid.*
131 *Ibid.*
132 *Ibid.*
133 Under s 2 of the Cybercrime Act, 'use' means that a person uses a computer program if they copy or move the computer program to a different location in the computer system or computer data storage medium in which it is held or to any other computer data storage medium; cause a computer program to perform any function; or obtain the output of a computer program. A person uses data, if the person copies or moves the data to a different location in the computer system or computer data storage medium in which it is held or to any other computer data storage medium; or obtains the output of data.

Section 3(1) creates an offence for the unlawful and intentional interception of data, but it is not only the act of intercepting but also the possession of data or the output of data, with the knowledge that such data was intercepted unlawfully, which deems an individual guilty of an offence.[134] Section 3(4) delineates data interception as the act of acquiring, viewing or copying data of a non-public nature using hardware, software or any other method to make the data available to someone other than its lawful owner, sender, recipient or intended recipient. This encompasses examining or inspecting data content and diverting data, in whole or in part, from its intended destination to another destination. If found guilty, section 19(2) sanctions include a fine, imprisonment for up to ten years, or both.

Section 3(3) criminalises the possession of data, where there is a reasonable suspicion that such data was intercepted unlawfully, and the possessor is unable to give a satisfactory exculpatory account of where they got the data from. An individual convicted may face a fine, imprisonment for up to five years, or both, as per the sentencing provisions outlined in section 19(1).

Section 4(1) prohibits the intentional use or possession of software or hardware tools which are used in the commission of cybercrime. This poses challenges to law enforcement due to their frequent dual-purpose nature, where use or possession may not be inherently unlawful. To avoid over-criminalisation, the act sets out specific intent as a requirement for conviction.[135] Software or hardware tools refers to any electronic, mechanical or other instrument, device, equipment, apparatus or a substantial component thereof, or computer program, primarily designed or adapted for the purpose of accessing, intercepting data, interfering with data or a computer program, interfering with a computer data storage medium or a computer system or acquiring, providing or utilising a password, access code or similar data or devices.[136]

For contravening section 4 there are fines, or imprisonment for up to ten years, or both.[137]

Section 5(1) criminalises the unlawful interference with data or a computer program. Interference with data or a computer program is defined as permanently or temporarily deleting, altering, rendering data or a computer program vulnerable, damaged or deteriorated; rendering data or a computer program meaningless, useless or ineffective; obstructing, interrupting or interfering with the lawful use of data or a computer program; or denying access to data or a computer program.[138]

Section 6(1) prohibits the unlawful intentional interference with a computer data storage medium or a computer system. This means an intentional alteration to any resource of, or interruption or impairment to the functioning, confidentiality, integrity or the availability of a computer data storage medium or a computer system. On conviction for contravening either sections 5(1) or 6(1), the sentencing provisions in section 19(2) provide for a fine or imprisonment for a period not exceeding ten years or both.

Passwords, access codes and similar data or devices have a specific function, which is to protect against unauthorised access to or the unauthorised use of or interference with data, a computer program, a data storage medium or a computer system for criminal purposes.[139]

Section 7(1) creates an offence for the unlawful and intentional acquisition, possession, provision to another person or use of a password, an access code or similar data or device. For this the penalty, detailed in section 19(2) is a fine, or imprisonment for a period not exceeding ten years, or both a fine and imprisonment.

Section 7(2) extends the criminalisation to the possession of passwords, access codes and similar data or devices, in respect of which there is a reasonable suspicion that it was acquired, possessed, is to be provided to another person or was used where such person is unable to provide a satisfactory exculpatory account of their possession. Here, the penalty is a fine, or imprisonment for a period of five years, or both.[140]

The next set of cybercrimes are categorised by Watney as offences committed or facilitated by means of data, computer programs, computer data storage and computer systems or computer-assisted crimes. This category criminalises traditional crimes that are facilitated by means of ICT.[141]

Section 8 sets out the statutory offence of cyber fraud, where a person unlawfully and with an intention to defraud makes a misrepresentation by means of data or a computer program; or through any interference with data or a

134 See s3(2) of the Cybercrime Act.
135 See n 83 above, 479.
136 See s 4(2) of the Cybercrime Act.
137 See s 19(2) of the Cybercrime Act.
138 See s 5(2) of the Cybercrime Act.
139 See n 83 above, 480.
140 See s 19(1) of the Cybercrime Act.
141 See n 83 above, 480.

computer program or interference with a computer data storage medium or a computer which causes actual prejudice; or is potentially prejudicial to another person. Phishing or pharming scams and email spoofing would amount to cyber fraud.[142]

Section 9(1) states that an individual who unlawfully creates false data or a false computer program with the intent to defraud, resulting in actual or potential harm to another person, is guilty of cyber forgery. Cyber uttering, as described in section 9(2), involves unlawfully passing off false data or a false computer program with the intent to defraud, resulting in actual or potential harm to another person, and is considered an offence.

Section 10 seeks to criminalise cyber extortion. This prohibition applies when an individual commits the offence of obtaining protected data; interfering with data or a computer program; interfering with a computer or computer system; or obtaining or using a password, access code or related data or devices, and threatens another person with the commission of such offences to gain an advantage from that person or to compel them to perform or abstain from performing any act.

Section 12 provides that the common law offence of theft must be interpreted so as to include the theft of an incorporeal asset.

Watney's third category of cybercrimes provides for aggravated offences. The objective of this category of offences is to protect essential computer systems and life, limb, property, essential services, the economy or the interests of the country, against criminal conduct in cyberspace pertaining to a restricted computer system.[143]

For this, section 11(1)(b) sets out that a restricted computer system means 'any data, computer program, computer data storage medium or computer system under the control of, or exclusively used by (i) any financial institution; or (ii) an organ of state as set out in section 239 of the Constitution [...] including a court'.

The offences set out in section 11(1) include the acquiring of protected data, interfering with data, a computer program, computer data storage medium or a computer system; crimes committed against a restricted computer system are regarded as aggravated offences, which are punishable with a fine or imprisonment of up to 15 years, in accordance with section 19(2).

Section 11(2) provides that the offences of interfering with data, a computer program, computer data storage medium or a computer system or cyber extortion that endanger life, or violate the physical integrity or physical freedom of, or causes bodily injury to, any person, or any number of persons; causes serious risk to the health or safety of the public or any segment of the public; causes the destruction of or substantial damage to any property; causes a serious interference with, or serious disruption of an essential service, facility or system, or the delivery of any essential service; causes any major economic loss; creates a serious public emergency situation; or prejudices the security, the defence, law enforcement or international relations of the Republic of South Africa, is guilty of an aggravated offence.

In part II, sections 14 to 16 criminalise the distribution of data messages that are harmful. It refers to offences that centre on the content of computerised communication itself. Part II must be read with part VI, which provides for orders to protect a complainant from the harmful effect of malicious communications and if these orders are violated, it constitutes a crime.[144]

The following forms of malicious communications constitute crimes, that is, communications that:

- incite damage to any property or violence by means of an electronic communication service (section 14);
- threaten persons with damage to property or violence against a person or a group of persons (section 15); and
- disclose an intimate image through a data message of a person without consent from the person photographed (section 16(1)). According to section 16(2) an 'intimate image' is defined as a portrayal, whether real or simulated, created by any means, in which a person is depicted as nude, with their genital organs or anal region exposed, or, if female, with their breasts displayed. It also encompasses instances where the covered genital or anal region or breasts are displayed in a manner that violates or undermines the individual's sexual integrity or dignity. Importantly, the person depicted must have had a reasonable expectation of privacy at the time the data message containing the image was made.

142 *Ibid,* 481.
143 *Ibid,* 481.
144 *Ibid,* 482.

Any person who is convicted of the abovementioned crimes is liable to a sentence of a fine or imprisonment for a period not exceeding three years or both a fine and imprisonment.[145]

In part III, any person who unlawfully and intentionally attempts; conspires with any other person; or aids, abets, induces, incites, instigates, instructs, commands or procures another person, to commit an offence in terms of part I or part II of this chapter, is guilty of an offence and liable on conviction to the punishment to which a person convicted of actually committing that offence would be liable.[146]

In part IV, section 18 provides for competent verdicts. The section provides exactly which crimes an accused person may be convicted of if the crime the individual is charged with is not proven (referred to as competent verdicts). For example, under section 18(1) it is stated that '…if the evidence in criminal proceedings does not prove the commission of the offence charged but proves a contravention of section 17 in respect of the offence charged; or in respect of any other offence of which an accused may be convicted on the offence charged, the accused may be found guilty of the offence so proved'.

In part VI, sections 20–23, orders to protect a complainant from the harmful effect of the different forms of malicious communications are provided for. This must be read in conjunction with part II, which provides for different forms of harmful malicious communications. This is in addition to the orders that are possible under the Protection from Harassment Act 17 of 2011.[147]

Section 20 provides for an interim protection order pending the finalisation of criminal proceedings. In accordance with section 20(1), a complainant who lays a charge with the South African police that an offence in terms of sections 14, 15 or 16 has allegedly been committed against them, may on an *ex parte* basis in the prescribed form and manner, apply to a magistrates court for an order pending the finalisation of the criminal proceedings to prohibit any person from further making available, broadcasting or distributing the data message or order an electronic communications service provider or person in control of a computer system to remove or disable access to the data message in question.

Section 21 provides that a communications service provider or a person in control of a computer system must furnish particulars to the court, such as the electronic communications identity number from where the data message originated; the name, surname, identity number and address of the person to whom the electronic communications identity number has been assigned; any information that indicates that the data message was or was not sent from the electronic communication identity number of the person to the electronic communication identity number of the complainant; and any other information that is available to an electronic communications service provider or a person in control of a computer system that may be of assistance to the court to identify the person who made available, broadcasted or distributed the data message in question or the electronic communications service provider or person in control of a computer system that provides a service to the person who made available, broadcasted or distributed that message.

Chapter 4 of the Cybercrime Act provides in sections 25–45 for the powers to investigate, search, access or seize certain items.

Chapter 5 of the Act provides in sections 46–51 for mutual assistance and sharing of information relevant to law enforcement agencies of foreign countries, where the disclosure of such information may assist the foreign country in carrying out investigations or may lead to cooperation with the foreign country to carry out an investigation. It also provides for a process for foreign requests for assistance and cooperation.

Chapter 7 of the act provides for evidence in section 53. It is important that evidence is gathered in such a manner that it complies with the admissibility requirements.

Q 5. Is there any case law or are there any decisions by a regulator regarding cyber incidents in your jurisdiction?

Under POPIA, various enforcement notices have been issued for security breaches around personal data.

145 See s 19 of the Cybercrime Act.
146 See s 17 of the Cybercrime Act.
147 See s 2 of the Harassment Act.

Q 6. Are there any upcoming policies, strategies or regulations that will impact cybersecurity in the metaverse?

The Department of Justice and Constitutional Development first published a Bill on 28 August 2015 on cybercrime and cybersecurity, updated it on 19 January 2017 and introduced it to Parliament on 22 February 2017. There were extensive comments on the bill during the public participation period in 2017. Those comments were considered and incorporated into a new bill that was published in October 2018. In 2018, a decision was made to separate the Cybercrimes Bill from the Cybersecurity Bill and, thus, in 2020 we got the Cybercrimes Act 19 of 2020. The Cybersecurity Bill is still making its way through the legislative process.

Bibliography

Legislation

The Constitution of the Republic of South Africa of 1996.

The Standards Act 8 of 2008.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA).

The Promotion of Access to Information Act 2 of 2000 (PAIA).

The Protection of Personal Information Act 4 of 2013 (POPIA).

The Critical Infrastructure Protection Act 8 of 2019 (the CIP Act).

The Cybercrime Act 19 of 2021.

The Minimum Information Security Standards of 1996 (MISS).

The National Cybersecurity Policy Framework (NCPF) of 4 December 2015.

The Department of Public Service's Directive on Public Service Information Security (2022).

The Department of Public Service's Directive on Cloud Computing in the Public Service (2022).

Cases

AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others 2021 (3) SA 246 (CC).

Books

Sylvia Papadopoulos and Sizwe Snail Ka Mtuze, *Cyberlaw@SA: The Law of the Internet in South Africa* (4th edn, Van Schaiks 2022).

Elizabeth De Stadler, Ilze Luttig Hattingh, Paul Esselaar and Jessica Boast, *Overthinking the Protection of Personal Information Act* (Juta 2022).

Yvonne Burns and Ahmore Burger-Smidt *Protection of Personal Information: Law and Practice* (2nd edn, Lexis Nexis 2023).

Websites

The National Cybersecurity Policy Framework (NCPF) (2015) 14, www.gov.za/sites/default/files/gcisdocument/201512/39475gon609.pdf, accessed 10 March 2024.

The Minimum Information Security Standards of 1996 (MISS), www.sita.co.za/sites/default/files/documents/MISS/Minimum%20Information%20Security%20Standards%20(MISS).pdf, accessed 10 March 2024.

www.dpsa.gov.za/dpsa2g/documents/ogcio/2022/egov_21_06_2022_directive.pdf, accessed 4 April 2024.

www.dpsa.gov.za/dpsa2g/documents/egov/2022/egovernment_02_02_2022.pdf, accessed 4 April 2024.

Nathan-Ross Adams Michalsons Attorneys, 'Directive On Cloud Computing In The Public Service | DPSA' (2022), www.michalsons.com/blog/directive-on-cloud-computing-in-the-public-service-dpsa/55782, accessed 4 April 2024.

Mbanjwa Michalsons Attorneys, 'Directive on Public Service Information Security | DPSA' (2022), www.michalsons.com/blog/directive-on-public-service-information-security-dpsa-2/59833, accessed 4 April 2024.