THE CONVERGENCE OF LEGISLATION ON CYBERCRIME AND DATA PROTECTION IN SOUTH AFRICA:

A Practical Approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013

Sizwe Snail ka Mtuze*
Adjunct Professor in Cyberlaw / ICT Law, Nelson Mandela University and Visiting Professor, The Center for Technology & Society (CTS), FGV School of Law

SUMMARY

This article seeks to give a historical background to the development of cybercrime laws in South Africa. It commences with a discussion on the common-law position regarding cyber-criminality then the article goes on to discuss the Electronic Communications Transactions Act (ECT) and the new Cybercrimes Act. This is followed by a discussion on Protection of Personal Information Act (POPIA) and same converges with the Cybercrimes Act, as well as the POPIA.

* LLB(UP), LLM (SA), Admitted Attorney - South African High Court, is an author and co-editor of the published *Cyberlaw @ SA III: The Law of the Internet in South Africa* (2012), as well as *Cyberlaw @ SA IV* published in January 2022. Sizwe was also a part-time Member of the Information Regulator (2016–2022) and also formed part of the Ministerial Advisory Group that assisted the Department of Justice and Constitutional Development in drafting and amending the Cybercrimes Act through its different stages of drafting. The author wishes to thank Mr Vilimile Gumede (Snail Attorneys) who has assisted with the technical editing of this article.

1 INTRODUCTION: BRIEF HISTORY OF LEGISLATION ON CYBERCRIME AND DATA PROTECTION

This article is a continuation of an article published by the writer in 2009.[1] The previous article was a discussion of the South African legal position *vis-à-vis* cybercrime and cybersecurity. It provided the common-law position prior to the enactment of the Electronic Communications and Transactions Act (ECTA),[2] and gave an exposition of the law's solution to the most pressing cybersecurity concerns at the time, which included hacking, cracking and phishing, among various other unlawful activities.[3]

At least 54 cyber-incidents were reported in the period between 1994 and 2016.[4] These included: hacking of the South African Police Service, which resulted in the release of details of thousands of whistle-blowers and victims; vulnerabilities on the portals of Vodacom and Cell C (mobile telephone network operators); a compromise of the State's Government Communication and Information System (GCIS); targeted hacks on Absa Bank resulting in the loss of R500 000.00; the duplication of Vodacom SIM cards for the purpose of intercepting One-Time-Pins (OTP) through phishing, which resulted in the theft of more than R7 000 000.00; and many more well-publicised cyber-attacks.[5]

Increased internet activity on social networks, e-governance, commercial services and the Internet of Things (IOT) has amplified the vulnerability of persons, as well as that of countries to cybercriminal activities.[6]

Offences that were created and regulated in terms of the common law and ECTA have now been codified in the Cybercrimes Act.[7] The legal framework regulating cybercrimes sets out the manner in which the different offences are dealt with in terms of the law.[8] The sentences imposed for the commission of cybercrimes are also set out in the Act.[9]

---

1 Snail "Cyber Crime in South Africa: Hacking, Cracking, and Other Unlawful Online Activities" 2009 1 *Journal of Information, Law & Technology* (*JILT*), http://go.warwick.ac.uk/jilt/2009_1/snail (accessed 2021-06-22).

2 25 of 2002.

3 Hayes "Computer Security Threats: Small Business Professionals' Confidence in Their Knowledge of Common Computer Threats" 2012 3 *Advances in Business Research* 107. In this paper, viruses, Trojans, spyware, malware and phishing were identified as the most common computer threats to businesses at the time.

4 Van Niekerk "An Analysis of Cyber-Incidents in South Africa" 2017 20 *African Journal of Information and Communication* https://doi.org/10.23962/10539/23573 (accessed 2021-06-22) 113–132.

5 Van Niekerk 2017 *AJIC* 118.

6 *Ibid.*

7 19 of 2020.

8 Dlamini "Understanding Policing of Cybercrime in South Africa: The Phenomena, Challenges and Effective Responses" 2019 5 *Cogent Social Sciences* https://doi.org/10.1080/23311886.2019.1675404 (accessed 2021-06-22).

9 S 19 of ECTA.

This article aims to achieve two objectives, the first of which is to provide a succinct update on recent developments in cybercrime law in South Africa. The second objective is to point out the convergence of cybercrime laws and data protection laws. The reason for this contribution is based on the critical claim that vulnerability is the common denominator between cybersecurity and data protection.[10]

The legal basis for data protection in South Africa is the protection of the right to privacy in terms of the Constitution.[11] This right has found application and interpretation in the courts.[12] The right to privacy, and more specifically the right to the protection of personal information, finds legislative protection in the Protection of Personal Information Act (POPIA).[13] This Act is appropriately discussed owing to the reality that cyberactivity raises concerns for the safety and security of personal information on the Internet.[14]

The legislature has acknowledged the need to protect personal information by including this piece of legislation in the country's laws on privacy. In doing so, there have been seven crucial acknowledgments. The first is that there is a need for regulation of how public and private bodies process personal information.[15] It is acknowledged that there is a need for the introduction of minimum conditions for the lawful processing of personal information.[16]

It is acknowledged that a data protection authority such as the Information Regulator serving as a custodian of the Act is an important instrument through which to achieve the Act's purpose,[17] as well as that of the Promotion of Access to Information Act (PAIA).[18] POPIA also acknowledges that there is a need for codes of conduct to be established in specialised industry sectors to ensure adequate and appropriate data protection measures.[19] The right of consumers not to be unlawfully targeted with unsolicited electronic communications and automated decision-making is also acknowledged,[20] as protected in terms of the Consumer Protection Act (CPA).[21]

It is acknowledged that there is a need to regulate the flow of personal information across the borders of the country;[22] and to lay a legal/legislative basis for regulating matters connected with all the aforementioned

---

10 Snail "Legal Intersections Between the Protection of Personal Information Act 4 of 2013 (POPIA) and the Cybercrimes Act 19 of 2020" (2021) CyberBrics Publications https://cyberbrics.info/legal-intersections-between-the-protection-of-personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/ (accessed 2021-06-22).

11 Constitution of the Republic of South Africa, 1996.

12 *Black Sash Trust v Minister of Social Development* 2017 (3) SA 335 (CC).

13 4 of 2013.

14 Kshetri "Cybercrime and Cybersecurity in Africa" 2019 *Journal of Global Information Technology Management* 22 77.

15 Ss 8–25 of POPIA.

16 *Ibid*.

17 Ss 39 and 40 of POPIA.

18 2 of 2000.

19 Ss 60 and 61 of POPIA.

20 Ss 69 and 71 of POPIA.

21 68 of 2008.

22 S 72 of POPIA.

concerns.[23] In light of these important acknowledgements, a discussion on data protection is pertinent. The reason for such a discussion in this article alongside a discussion on cybercrime is that, while these are two distinct areas of information communications technology (ICT) law, they are indeed related in that they present the law with an opportunity to remedy situations of vulnerability.

Vulnerability in the cybercrimes area takes various forms, such as fraud, forgery and uttering, whereas in the area of data protection, it may take the form of data breaches. This article therefore also intends to interrogate the current laws along this vein of vulnerability.

Activities that occur in the context of technology usage largely entail the sharing of data. The accessing, dissemination, transmission and processing of data often entail the reality that the nature of the data itself may often be private. This is to say that it may involve the processing of information such as: a person's identification number; symbol; email address; physical address; telephone number; location information; online identifier; information relating to the race, 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; and other forms of personal data.[24]

The common-law position on cybercrimes was given in the previous article by highlighting the fact that at common law it is not a cumbersome exercise to prove defamation, indecency, theft, forgery, and malicious damage to property in the form of malicious code such as viruses, worms and Trojan Horses, as well as unlawful monitoring and interception of data messages.[25] Case law has certainly developed since the enactment of ECTA.[26]

Prior to a detailed discussion, it is of value to give a brief synopsis of the current status of data protection law given that there is an intersection between these two areas of law and technology. This article discusses the manner in which the right to privacy has been interpreted and applied by the courts and demonstrates how cybercrime and data protection laws intertwine.

Watney provides a concise background and analysis of cybercrime law in South Africa,[27] noting that the nature of cyberspace is such that the commission of crimes across physical borders has become easier.[28] It is

---

23 These acknowledgements are embodied in the long title of POPIA.

24 S1 of POPIA.

25 The exposition on the common-law position was given by citing case law including *S v Van den Berg* 1991 (1) SACR 104 (T); *S v Harper* 1981 (2) SA 638 (D); *S v Manuel* 1953 (4) SA 523 (A) 526; and *S v Howard* (unreported case no. 41/258/02). Case law discussed prior to the enactment of ECTA includes *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A); *R v Douvenga* (District Court of the Northern Transvaal, Pretoria, case no 111/150/2003); *SB Jafta v Ezemvelo KZN Wildlife* (Case D204/07); and *S v Motata* Johannesburg District Court case number 63/968/07 (unreported).

26 See *Okundu v S* [2016] ZAECGHC 131 and *Mgoqi v S* [2020] ZAECGHC 33.

27 Papadopoulos and Snail *Cyberlaw @ SA IV* (2021) ch 13 463.

28 Papadopoulos and Snail *Cyberlaw @ SA IV* ch 13 470–472.

submitted that this forms one of the bases for the argument that there is a convergence in the law on cybercrimes and data protection, especially considering that data or information has become a valuable currency traded across the globe daily.

2 CYBERCRIME IN THE CONTEXT OF ECTA AND THE COMMON LAW

Considering that the previous article clearly drew on the developments in cybercrime law in the context of the common law and ECTA at the time, it is fitting that the article first discusses developments in case law on how the Act has found practical application. The provisions of ECTA are discussed here, and for the sake of relevance, the focus is on the provisions of the Act in its current form. It should be noted that the discussion on ECTA is on how the courts have applied and interpreted its provisions.

In the previous article, the common-law position on cybercrimes was given with reference to the common-law crimes of defamation, indecency (including online child pornography), *crimen injuria*, fraud, defeating the ends of justice, contempt of court, theft and forgery.[29] The legal position on such crimes was given by citing the case of *S v Howard*,[30] where the court found that causing an information system to break down is a scenario fit for classification as malicious damage to property.[31] Although there is no one general definition for cybercrime, ECTA has characterised cybercrime by providing that it is

> "any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems including any device or the internet or any one or more of them".[32]

Watney notes that cybercrime can be categorised as cyber-dependent crimes; cyber-enabled or cyber-assisted crimes; or computer-supported crimes.[33] Watney also importantly notes that the development of ICT regulation in the context of cybercrime has essentially entailed four phases.[34]

In the first phase, the Internet was not regulated; as a result, common-law offences were insufficient to deal with nuanced means of committing crimes in cyberspace. The second phase for South Africa began with the enactment of ECTA, which afforded some efficacy to law enforcement agencies and the criminal justice system to deal with cybercrimes. The third phase saw the

---

29 Snail http://go.warwick.ac.uk/jilt/2009_1/snail.

30 *S v Howard supra*.

31 The precise definition entails that a person may be found guilty of the crime of malicious damage to property "[i]f he unlawfully and intentionally damages property belonging to another; or his own insured property, intending to claim the value of the property from the insurer". See Snyman *Criminal Law* (2021) and the discussion there on *Mashanga* 1924 AD 11 12; *Bowden* 1957 (3) SA 148 (T) 150B; *Kgware* 1977 (2) SA 454 (O) 455; and *Mnyandu* 1973 4 SA 603 (N) 606A as referenced by the court in *Mokoena v S* [2020] ZAMPMHC 32 par 24.

32 Papadopoulos and Snail *Cyberlaw @ SA IV* ch 13 477.

33 *Ibid.*

34 *Ibid*.

enactment of supplementary legislation such as the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA),[35] the purpose of which was to regulate law enforcement surveillance.

It is, however, crucial to note that large portions of RICA have since been declared unconstitutional in the *AmaBhungane* case.[36] The fourth phase, as summarised by Watney, entails the enactment of comprehensive legislation dealing exclusively with cybercrime and related issues. This is the Cybercrimes Act.[37] Practical application of the Cybercrimes Act had not yet become a reality at the time of writing this article, but a number of court decisions on the basis of ECTA are explored in order to give a view of how these provisions have been tested in the courts.

In the case of *Okundu v S*,[38] the court upheld an appeal on sentence where the appellant had been convicted on various counts of contravening section 86(1), (3) and (4) of ECTA. The appellant had been convicted for unlawfully gaining access to the information of various persons to whom some banks had issued original cards, such information having been encoded on the magnetic strips of the original cards. The appellant had neither the authority nor the consent of the lawful cardholders and/or the banks to access the information.[39]

In the case of *Okundu v S*,[40] the court found that the appellant had committed an offence in terms of section 86(4) of ECTA, whose equivalent is section 8 of the Cybercrimes Act. This is the fraud provision, and it is important to note that the court interpreted it in the following manner:

> "Fraud consists in unlawfully making, with intent to defraud, a misrepresentation which causes actual prejudice or which is potentially prejudicial to another. The essential elements of fraud are: unlawfulness; making a misrepresentation; causing prejudice or potential prejudice and intent to defraud. The appellant was convicted on counts 1 to 5 because he unlawfully made misrepresentations to the banks with the intent to defraud them, which misrepresentations caused prejudice to them and/or the lawful cardholders."[41]

In the case of *Mgoqi v S*,[42] the court allowed an appeal and set aside the sentences imposed by a magistrates' court. The court found that the appellant had contravened section 86(1) of ECTA by unlawfully and intentionally gaining access to, or intercepting, data such as client information (encoded on magnetic strips of bank cards) of various

35 70 of 2002.

36 *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC* [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC).

37 19 of 2020.

38 *Okundu v S supra*.

39 *Okundu v S supra* par 6.

40 *Okundu v S supra*.

41 *Okundu v S supra* par 10 (footnotes omitted).

42 *Mgoqi v S supra*.

international financial institutions.[43] This provision of ECTA has been amended by section 3 of the Cybercrimes Act.

One of the aims of cybercrime legislation is to prohibit the unlawful overcoming of protection measures intended to prevent access to data transmitted to or from a computer system. In the case of *Myeni v S*,[44] the court dismissed an appeal by the accused where he had been convicted of having been a member of a syndicate that wrongfully and unlawfully used a device primarily designed to overcome security measures. The perpetrators, without the authority of the Koukamma Municipality, had used computer software by the name of Winspy that captures keystrokes in order to overcome security measures designed to protect data, namely computer usernames and passwords.[45] The court found the court *a quo*'s sentence to be appropriate.[46]

Section 86(5) of ECTA prohibits the unlawful and intentional interference with data or a computer program.[47] In the case of *Salzmann v S*,[48] the SCA found that an offence in terms of section 86(5) of ECTA is a serious one. In this case, a mobile service provider, Cell C, had suffered a cyber-attack perpetrated by the appellant. Before striking the matter off the roll, the court found:

> "Section 89 of the ECT Act prescribes a maximum sentence of a fine or imprisonment not exceeding five years for a contravention of s 86(5). The fact that the legislature found it necessary to place this offence on the statute book is in itself a clear indication of the prevalence of the unlawful hacking of others' computers and networks. The offence is by its very nature a severe one. It invades the privacy of others, something our law earnestly protects, and may have far reaching consequences. In the present case it affected some 80% of the network of a large mobile cellular operator, and it took a week to restore the mischief that had been done."[49]

The previous article alluded to and highlighted the fact that ECTA prohibits the unlawful and intentional acquisition, possession or provision of passwords, access codes or similar data to another person for the purposes of committing cyber fraud, cyber forgery, uttering and cyber extortion.[50] In *Mgoqi v S*,[51] the court considered that among the charges against the appellant was the accusation of forgery. The appeal court, however, found that the court *a quo* had erred in its finding. Section 87 of ECTA is the applicable provision, which was referred to thus:[52]

---

43 *Mgoqi v S supra* par 3.

44 *Myeni v S* [2018] ZAECGHC 107; 2019 (1) SACR 360 (ECG).

45 *Myeni v S supra* par 4.

46 *Myeni v S supra* par 29.

47 S 86(5) of ECTA provides: "A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence."

48 [2019] ZASCA 145; [2020] 1 All SA 361 (SCA); 2020 (2) SACR 200 (SCA).

49 *Salzmann v S supra* par 40.

50 Snail http://go.warwick.ac.uk/jilt/2009_1/snail.

51 *Mgoqi v S supra* par 35.

52 The court drew a distinction between forgery and fraud by citing *LAWSA* vol 11 3ed par 374, where it is stated: "Forgery is committed by unlawfully making a false document with intent to defraud to the actual or potential prejudice of another. It is a species of fraud. In forgery the misrepresentation takes place by way of the falsification of a document. Apart

> "In convicting the appellant for forgery the Magistrate did so on the basis that a plastic bank card constituted a document. This is evidenced by his reasoning that 'a plastic bank card which does not belong to you with your name printed on it and signature on the back is clearly forgery'. It is unnecessary to express a view on the correctness or otherwise of this finding. What was clearly overlooked by the Magistrate is that, by definition, the case for the State failed in one fundamental respect, namely that the intent to defraud was not proven."

In the case of *Fourie v Van der Spuy and De Jongh Inc*,[53] the court considered a dispute involving the hacking of emails and subsequent payments made to hackers who remained unknown. The relief sought by the applicant entailed requesting the court to order the respondents to be held jointly and severally liable for payment of an amount of R1 744 599.45. An important fact is that the respondents were a law firm and legal practitioners.[54] In considering the facts before it, the court took note of the case of *Jurgens v Volschenk*.[55] In *Jurgens*, the Eastern Cape Local Division made a cautionary finding for law practitioners by stating the following:

> "I do not dispute the doctrine that an attorney is liable for negligence and want of skill. Every attorney is supposed to be reasonably proficient in his calling, and if he does not bestow sufficient care and attention, in the conduct of business entrusted to him, he is liable; and where this is proved the Court will give damages against him."[56]

The court in *Fourie* found that there had been instances of fraud conducted by hackers that were unknown to any of the parties. The court nevertheless apportioned the damage suffered by the applicant to the respondents, having found specifically that the second respondent had failed to exercise the requisite skill, knowledge and diligence expected of an average practising attorney. It is submitted that instances such as the occurrences in *Fourie* are commonplace. For this reason, this discussion extends beyond the status of cybercrime regulation to include data protection as more fully discussed later in this article.

The adjudication of cybercrime in South Africa owes a debt not only to ECTA, but also to the Specialised Commercial Crimes Court, which was first established in Pretoria in November 1999.[57] The purpose of its

from this, all the requirements of the crime of fraud must be present, such as the intent to defraud and the actual or potential prejudice. However, whereas fraud is completed only when the misrepresentation has come to the notice of the representee, forgery is completed the moment the document is falsified. If the document is then brought to the attention of others, a separate offence is committed, namely uttering the document. Because the person falsifies the document is in most cases also the one who offers it to another, it has become customary to charge that person with both forgery and uttering, which are nevertheless two distinct offences."

53 [2019] ZAGPPHC 449; 2020 (1) SA 560 (GP).

54 *Fourie v Van der Spuy and De Jongh Inc supra* par 2.

55 *Ben Adrian Jurgens and Wendy Jurgens v Lynette Volschenk* (4067/18) ZAECHC (unreported).

56 *Ben Adrian Jurgens and Wendy Jurgens v Lynette Volschenk supra* par 20.

57 Albeker "Justice Through Specialisation? The Case of the Specialised Commercial Crimes Court" (2003) *Institute for Security Studies* https://www.files.ethz.ch/isn/118731/76% 20FULL.pdf (accessed 2021-07-12).

establishment was to unburden the criminal justice system and efficiently tackle various commercial crimes through a system of magistrates, prosecutors and other court officials specifically dedicated to the task. The role of this specialised court has also entailed an interpretation and application of the provisions of ECTA. In the case of *Msomi v S*,[58] the court considered an appeal from the Port Elizabeth Specialised Commercial Crimes Court, where the appellant had been charged with fraud in terms of ECTA and the Prevention of Organised Crime Act.[59] The court considered the prevalence of cyber fraud and made the following remarks regarding its effects:

> "It is so that there is unfortunately a misguided perception that these crimes are somewhat less morally reprehensible than fraud and theft committed in the 'old fashioned' way. This perception is unfortunately further encouraged by films in which cyber-criminals are portrayed as debonair and devil-may-care rebels who fight a lone and just battle against an evil system … The ability of cyber 'hackers' to infiltrate these electronic systems for their own selfish purposes consequently has far-reaching and deleterious consequences for the economy, both domestically and globally."

The body of laws regulating cybercrime prior to the enactment of the Cybercrimes Act extends beyond the provisions of ECTA and the Prevention of Organised Crime Act. In the case of *Prinsloo v S*,[60] the court had to make an appeal determination where the appellant had *inter alia* been charged in the court *a quo* with a contravention of the Films and Publications Amendment Act.[61]

The charge levelled against the appellant was that of "Importation or Procuring of Child Pornography".[62] A forensic cyber-analyst (expert) gave evidence to the court that the appellant's computer had been used to access child pornography, and that thereafter a software application had been used to remove child pornography from the appellant's computer a few hours prior to his arrest.[63] Having considered his version that third persons had downloaded such child pornography (without providing any names of the said persons), the court dismissed the appeal, finding that his version was filled with improbabilities and contradictions.[64]

The cases briefly explored in this article demonstrate that there have in fact been consequences for cybercriminals during the third phase of regulation. ECTA mainly addresses the unlawfulness of interfering with data or information, and it thus creates offences.[65] From the few reported cases decided on appeal in the high courts, it is clear that the lower courts have over the years exercised the function of interpreting and applying ECTA to practical scenarios where law enforcement agencies have preferred charges against cybercriminals in terms of section 86 of ECTA. The ECTA regime

---

58 [2019] ZAECGHC 80; 2020 (1) SACR 197 (ECG).
59 121 of 1998.
60 [2018] ZAFSHC 35.
61 3 of 2009.
62 *Prinsloo v S supra* par 1.
63 *Prinsloo v S supra* par 18.
64 *Prinsloo v S supra* par 45.
65 S 86(2) of ECTA.

has come to its end insofar as regulating cybercrimes is concerned. In its place, the Cybercrimes Act is now the key legislation that creates offences and penalties for cybercriminality. The provisions of the Cybercrimes Act are discussed in the next section of this article.

3 THE SALIENT PROVISIONS OF THE CYBERCRIMES ACT

The Preamble of the Cybercrimes Act states that its purpose entails the creation of offences that have a bearing on cybercrime and to prescribe penalties for such crimes.[66] Chapter 2 of the Cybercrimes Act has five substantive criminal law segments. Part I relates to cybercrimes that have been re-codified from existing crimes, as well as newly added offences. Part II relates to malicious communication crime. Section 2 of the Act provides that any person who unlawfully and intentionally secures access to data, a computer program, a computer data storage medium or a computer system is guilty of an offence.

Part III creates offences in the specific context of various cybercrime activities; these are attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring a person to commit offences specified in the Act. Part IV contains competent verdicts, which guide the courts in making their pronouncements on cybercriminality. Part V makes provision for orders that may be given by the courts in order to protect complainants from the harmful effects of malicious communications.

The Act is broken up into nine chapters. Chapter 1 is the definition and interpretation section (section 1). Chapter 2 comprises Parts I, II, III, IV and V as highlighted in the preceding paragraphs. Chapter 3 pertains to issues of jurisdiction. Chapter 4 of the Act sets out the powers to investigate, search, access or seize. Chapter 5 makes provision for mutual assistance between South Africa and foreign states. Chapter 6 makes provision for the establishment and functions of a "designated point of contact".

Chapter 7 provides for the adducing of evidence by way of sworn statements. Chapter 8 provides for reporting obligations of electronic communications service providers and financial institutions and building capacity to police cybercrimes. Chapter 9 contains general provisions, including on the authority of the executive authority to enter into agreements; the repeal and amendment of certain laws; the inclusion of regulations; and the commencement of the Act. For the purpose of practicality, the discussion contained in this article is detailed insofar as Parts I and II of Chapter 2 are

[66] The Cybercrimes Act makes amendments to 11 critical pieces of legislation. These are the Criminal Procedure Act 51 of 1977; the South African Police Services Act 68 of 1995; the Films and Publications Act 65 of 1996; the Criminal Law Amendment Act 105 of 1997; the National Prosecuting Authority Act 32 of 1998; the Correctional Services Act 111 of 1998; the Financial Intelligence Centre Act 38 of 2001; the Electronic Communications and Transactions Act 25 of 2002; the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002; the Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007; and the Child Justice Act 75 of 2008.

concerned, but is rather limited on the rest of the Act. The reason is that the creation of the offences as well as the consequences thereof are the most pertinent areas of concern in the wake of the Cybercrimes Act having been recently enacted at the time of writing this article. On 1 June 2021, the President of the Republic of South Africa signed the Cybercrimes Act into law. In accordance with this specialised legislation, there are now procedures created to cater for investigation of Cybercrime and co-operation of multinational law enforcement agencies -fostering multi-agency collaboration. Chapter 2 of the Cybercrimes Act has two substantive criminal law segments, namely Part I on cybercrimes (which has re-codified existing crimes and added new offences) and Part II on malicious communication crimes. The President signed a Presidential Minute indicating that the commencement date of the Cybercrimes Act will be 1 December 2021. The following sections, however, will not yet commence namely:

- Part VI of Chapter 2 which deals with issuing of protection orders which can be granted against suspected cyber harassment, cyber threats of damage to property or anyone inciting others to damage property, and revenge porn. Section 20(1) of the Cybercrimes Act provides that a complainant who lays a charge with the South African Police Service (SAPS) that an offence contemplated in s 14, 15 or 16 has allegedly been committed against them, may, on an *ex parte* basis, apply to a magistrate's court for a protection order, pending the finalisation of the criminal proceedings.
- Section 38(1)*(d)–(f)* which provides for any person who unlawfully or intentionally gives false information under oath or by way of affirmation knowing it to be false or not knowing it to be true, with the result that an expedited preservation of data direction contemplated in s 41 is issued or a preservation of evidence direction contemplated in s 42 is issued; or a disclosure of data direction contemplated in s 44 is issued, is guilty of an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding two years or to both such fine and imprisonment.
- Section 40(3) provides that an electronic communications service provider who is required[67] to provide an electronic communications service which has the capability to store communication-related information and not required to store communication-related information in terms of a directive issued in terms of s 30(2) of the Cybercrimes Act must, in addition to any other obligation imposed by any law, comply with a real-time communication-related direction in terms of which the electronic communications service provider is directed to provide real-time communication-related information in respect of a customer, on an ongoing basis, as it becomes available.
- The non-commencement also applies to the direction for expedited preservation of data as contemplated in s 41 of the Cybercrimes Act, in terms of which the electronic communications service provider is directed to preserve real-time communication-related information in respect of a customer, and s 42 of the Cybercrimes Act which deals with

[67] S 30(1)*(b)* of the Regulation of Interception of Communications and Provision of Communication-related Information Act.

preservation of evidence direction in terms of which the electronic communications service provider is directed to preserve real-time communication-related information in respect of a customer.

- The non-commencement will apply to a disclosure of data direction contemplated in s 44 of the Cybercrimes Act, in terms of which the electronic communications service provider is directed to provide real-time communication-related information in respect of a customer that was preserved or otherwise stored by the electronic communications service provider or any order of the designated judge in terms of s 48(6) of the Cybercrimes Act in terms of which the electronic communications service provider is ordered to obtain and preserve any real-time communication-related information; or obtain and furnish traffic data.
- Section 54 of the Cybercrimes Act which provides that an electronic communications service provider must, within 72 hours of having become aware, report an offence committed in terms of Part I of the Act to the SAPS will also not commence. The remainder of the Act will apply save for the exclusion of ss 11B, 11C, 11D and s 56A(3)*(c)–(e)* of the Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007 in Chapter 9 in the schedule of laws repealed by s 58 of the Cybercrimes Act.

In this article, the discussion focuses on unlawful and intentional access;[68] unlawful interception;[69] unlawful acts in respect of software/hardware tools; interference with data;[70] interference with data or computer programs;[71] unlawful interference with storage mediums;[72] unlawful acquisition, possession, provision, receipt or use of passwords, access codes or similar data/device(s); aggravated offences in terms of the Act;[73] theft of incorporeal property;[74] malicious communications including incitement to violence or causing damage to property;[75] revenge pornography;[76] and attempting, conspiring, aiding, abetting, inducing, inciting, instigating, and instructing or procuring another to commit a criminal offence.[77] The discussion of the provisions of the Cybercrimes Act ends with consideration of sentencing for offenders found guilty of having committed cybercrimes,[78] as well as of court orders to protect complainants during the course of criminal proceedings.[79]

68 S 2 of the Cybercrimes Act.
69 S 3 of the Cybercrimes Act.
70 S 4 of the Cybercrimes Act.
71 S 5 of the Cybercrimes Act.
72 S 6 of the Cybercrimes Act.
73 S 7 of the Cybercrimes Act.
74 S 12 of the Cybercrimes Act.
75 Ss 13, 14 and 15 of the Cybercrimes Act.
76 S 16 of the Cybercrimes Act.
77 S 17 of the Cybercrimes Act.
78 S 19 of the Cybercrimes Act.
79 S 20 of the Cybercrimes Act.

3 1 Offences against confidentiality, availability, data, computer systems and storage data

Section 2 of the Act makes provision for an offence in relation to the unlawful securing of access in respect of a computer system or a computer storage medium. This section provides that any person who unlawfully and intentionally secures access to data, a computer program, a computer data storage medium or a computer system is guilty of an offence. For example, a cybercriminal might obtain software such as eBlaster,[80] which may be used to gain access to an organisation's bank account for illicit and illegal purposes such as siphoning off funds.[81]

Section 3 of the Act creates an offence in the event of unlawful interception of data, which may take the form of wire-tapping, installing a sniffer to monitor communications on a network, and packet sniffing.[82] In the case of wire-tapping, electronic equipment may be used to monitor communications between two separate computers, while a sniffer is defined as "[a] program that monitors data that are sent via a network".[83] Watney defines surveillance broadly and generally as "to watch over", and defines monitoring specifically as "the listening to and/or reading of the content of communication". Considering that such a technical term is not specifically defined in the Act itself, it is important to view section 3 in light of available literature and other legislation such as RICA, where the definition of "monitor" "includes to listen to or record communication by means of a monitoring device".

Section 4 of the Act creates an offence in the event that a person unlawfully and intentionally uses or possesses any software or hardware tool whose purpose is to contravene sections 2(1) or (2), 3(1), 5(1), 6(1), or 7(1)(*a*) or (*d*). An interesting feature of this section is that it makes it unlawful not only to make use of such a software or hardware tool, but also simply to be in possession of such a tool. In this context, great caution and vigilance ought to be exercised by any person making use of digital technologies, considering that legally it is *prima facie* immaterial whether unlawful software or hardware tools in one's possession are subject to unlawful use by another.

Section 5 of the Act creates an offence in the event that a person unlawfully and intentionally interferes with data or a computer program. It is important to note that the Act provides some guidance in that this section

---

80 See Dinan "Ware-Withal: EBlaster the Ultimate Tool of the Spies Who Love You" (2003) *Boston Business Journal* https://www.bizjournals.com/boston/blog/mass-high-tech/2003/06/ware-withal-eblaster-the-ultimate-tool-of.html (accessed 2021-07-13): "Sign on for eBlaster and you'll get hourly reports detailing every keystroke typed by your kids, husband, wife, sweetheart or employees. You'll be able to read both sides of their e-mail conversations via Hotmail, Yahoo, AOL, Microsoft Outlook and EarthLink. Both sides of all instant messages and back-and-forth from inside chat rooms is reported in detail, including chat with providers AOL and MSN Instant Messenger."

81 Papadopoulos and Snail *Cyberlaw @ SA IV* ch 13 477.

82 Maat *Cybercrime: Unauthorised Interception* (2009) ch 6. See also Van der Merwe *Computers and the Law* (2000) 169; and Gordon "Internet Criminal Law" in Buys (ed) *Cyberlaw @ SA* (2000) 428.

83 *Ibid*.

provides a tailored definition of what constitutes interference. The Act accordingly provides that deleting, altering, rendering vulnerable, damaging, deteriorating, rendering meaningless, useless or ineffective, obstructing, interrupting or interfering with the lawful use, or denying access to data or a computer program falls within the scope of "interference".[84]

The Act is clearly wide enough to include any number of such actions, and it is submitted that the Act affords greater protection to victims of cybercrime in this way. The tailored definition of "interference" provided for by the legislature is likely to ensure legal certainty for the courts when dealing with cyber-interferences of various natures. Watney makes it clear that privacy on the Internet entails the privacy of communications. She characterises communications privacy as protection against interference and intrusion regarding communications that occur on websites visited, as well as in electronic mails sent and received.[85]

Section 6 of the Act creates an offence in the event that a person unlawfully and intentionally interferes with a computer's data storage medium or a computer system. As in section 5, section 6 provides a clear definition of what constitutes an interference in this context. In terms of section 6, an interference with a computer data storage medium or a computer system has occurred where there is: either a permanent or temporary alteration of any resource; or an interruption or impairment to the functioning, confidentiality, integrity or availability of the medium or system.[86] It is therefore submitted that the legislature has apparently considered the various eventualities of interference as tested by the courts and reported by law enforcement agencies, and accordingly resolved to provide a comprehensive definition for "interference" in this particular context.

3 2 Malicious computer-related crimes

Sections 7, 8, 9 and 10 of the Act respectively create offences in the event that a person unlawfully and intentionally acquires, possesses, provides to another person, or uses a password, an access code or similar data or device (section 7) for purposes of committing cyber fraud (section 8), cyber forgery, uttering (section 9) and cyber extortion (section 10).[87]

There is a clear distinction between cybercrimes and common-law offences such as fraud, forgery and extortion in that the Cybercrimes Act links the former directly to the use of data and a computer or computer program.[88] It is therefore submitted that the scope and application of the

[84] S 5(2) of the Cybercrimes Act.

[85] Watney "The Evolution of Internet Legal Regulation in Addressing Crime and Terrorism" 2007 *The Journal of Digital Forensics, Security and Law* 2 40.

[86] S 6(2) of the Cybercrimes Act.

[87] Ss 7, 8, 9 and 10 of the Cybercrimes Act.

[88] For e.g., in *Van Heerden v S* [2016] ZAFSHC 191, the court gave the common-law definition of fraud by stating that "[f]raud is the unlawful and intentional making of a misrepresentation which causes actual prejudice, or which is potentially prejudicial to another". See *Hattingh v S* [2016] ZAWCHC 199 in respect of the common-law definition of forgery; *Ndlovu v S* 2016 ZAECBHC 12 for a characterisation of the common-law crime of

Cybercrimes Act in relation to these crimes *prima facie* seems sufficiently suited to the context of crimes committed in conjunction with data and/or computers. It is also submitted that the Cybercrimes Act, as a more comprehensive piece of legislation, has cured possible deficiencies in the wording used in ECTA.

3 3 Aggravated offences

Section 11 of the Act provides for aggravated offences and maps out clearly that its application extends to sections 3(1), 5(1), 6(1) or 7(1) insofar as the passwords, access codes or similar data and devices are concerned. The guilt assigned to an infringer/perpetrator in this context is strict in that where such a person knows or ought reasonably to have known/suspected that the computer system is restricted, they may be found guilty of an aggravated offence. The Act goes a step further by providing a succinct definition of a "restricted computer system".[89]

Section 11 provides that any data, computer program, computer data storage medium or computer system under the control of, or exclusively used by a financial institution or an organ of state as set out in section 239 of the Constitution falls within the meaning of "restricted computer system".[90] Accordingly, the unlawful interception of data, unlawful interference with data or a computer program, unlawful interference with a computer data storage medium or computer system, or unlawful acquisition, possession, provision receipt or use of a password, access code or similar data or device of a financial institution (that is, one of the main banking institutions) or a government ministry qualifies as an aggravated offence.[91] Watney notes that the South African common law lacked the requisite flexibility to regulate cybercrimes that had not existed before the Internet became a reality. In giving a detailed discussion on cybercrime regulation in the Act, she makes the point that the Act does indeed afford greater protection.[92]

Section 12 of the Act is a rather straightforward and easy-to-comprehend provision; it holds: "The common law offence of theft must be interpreted so as not to exclude the theft of incorporeal property." This provision therefore prescribes that the theft of incorporeal property is included in the common-

extortion; and *Cossie v S* [2011] ZAFSHC 169 in respect of the common-law crime of uttering.

89 S 1 of the Cybercrimes Act.

90 S 1 of the Cybercrimes Act defines a financial institution as one: "defined in section 1 of the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017)." S 1 of the Financial Sector Regulation Act 9 of 2017 defines a financial institution as any of the following, other than a representative: "(*a*) A financial product provider; (*b*) a financial service provider; (*c*) a market infrastructure; (*d*) a holding company of a financial conglomerate; or (*e*) a person licensed or required to be licensed in terms of a financial sector law." S 239 of the Constitution provides that: "'organ of state' means – (a) any department of state or administration in the national, provincial or local sphere of government; or (b) any other functionary or institution – (i) exercising a power or performing a function 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, but does not include a court or a judicial officer".

91 Papadopoulos and Snail *Cyberlaw @ SA IV* ch 13 481.

92 *Ibid.*

law offence of "theft", The court in *Van Heerden v S*[93] affirmed the following definition:

> "A person commits theft if he unlawfully and intentionally appropriates moveable, corporeal property which
>
> (a) belongs to, and is in the possession of, another; (b) belongs to another but is in the perpetrator's own possession; or (c) belongs to the perpetrator but is in another's possession and such other person has a right to possess it which legally prevails against the perpetrator's own right of possession
>
> provided that the intention to appropriate the property includes an intention permanently to deprive the person entitled to the possession of the property, of such property."

The legal distinction between corporeal and incorporeal property has been characterised in the following manner by Njotini:[94]

> "Pre-classical Roman law was a further development of old Roman law. This law classified property into corporeal things or *res corporales* and things incorporeal or *res incorporales*. Corporeal things referred to tangible objects. The examples were land, a slave, a garment, gold and silver. Incorporeal things were intangible objects, for example an inheritance, usufruct, obligation or servitude. The last-mentioned things had the quality of being rights over property … Pre-classical and classical Roman law extended the interests in property to both corporeals and incorporeals. Importantly, the view in classical Roman law was that corporeals and incorporeals must be of economic value to a person. In other words, a person had to have an interest in property, which was calculated to be economic in nature."

Section 14 of the Act creates an offence in the event that a person discloses, by means of an electronic communications service, a data message to a person, group of persons or the general public with the intention to incite damage to property that belongs to, or violence against, a person or group of persons. This section demonstrates the necessity for a piece of legislation suited specifically to acts committed in cyberspace as opposed to incitement as understood and interpreted at common law.

There is a distinction between sections 14 and 15 of the Act. Section 15 creates an offence where a person unlawfully and intentionally discloses a data message that *threatens* a person with damage to property belonging to that person or a related person, or with violence against that person or a related person. Merely making the threat of damage to property or violence is punishable as an offence.

Section 16 of the Act has the title "Disclosure of data message of intimate image" and creates an offence in the event that a person unlawfully and internationally discloses, by means of an electronic communications service, a data message of an intimate image of a person without the consent of such person. The Act specifically sets the parameters within which an intimate image can be perceived. This provision stretches to include real and simulated images of a person depicted nude, or where the bare or covered

93 *Van Heerden v S supra* par 6, where the court cited Snyman *Criminal Law* (2008) 483.

94 Njotini "Examining the 'Objects of Property Rights': Lessons from the Roman, Germanic and Dutch Legal History" 2017 *De Jure* 1.

genital organs or anal region, or the breast area of a female, transgender or intersex person, are depicted.[95]

On 4 May 2021, a person identified in the media as Hazel Mahazard allegedly posted a nude photo of a popular deejay, Kabelo Motsamai (popularly known as Prince Kaybee).[96] The media thereafter reported that the alleged victim issued a letter demanding a public apology, failing which legal steps would be taken by Mr Motsamai. It is submitted that such a scenario would invoke the section 16 provision, and that courts are likely to test such scenarios in future since "revenge pornography" has become common.[97]

Section 17 of the Act creates an offence in the event that a person 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 set out in Parts I or II of Chapter 2 of the Act. This provision may be interpreted to mean that not only are there consequences for persons who carry out cybercrimes in terms of the Act, but also for persons who act as accomplices, or persons who give commands and instructions for cybercrimes to take place.

Musoni relies on Bloom's characterisation of revenge pornography, which was:

> "Non-consensual pornography/involuntary pornography, involves the distribution of sexually graphic images of an individual where at least one of the individuals depicted did not consent to the dissemination."[98]

In her discussion, she makes reference to the Cybercrimes Act in its pre-enactment phase (as a Bill), highlighting the importance of the element of consent.[99] Musoni agrees that there is a world of difference between pornography in its ordinary sense and meaning and revenge pornography, which is created by the element of lack of consent in the latter.

Musoni also points out that the Act makes provision for consequences only for the original perpetrator who first disseminates the sexually graphic images, but not for any subsequent sharing by third parties.[100] While the Cybercrimes Act falls short in this regard, POPIA certainly creates offences for non-compliance with POPIA in that the definition of personal information is non-exhaustive: "Personal information means information relating to an identifiable, living, natural person".[101]

It is submitted that by virtue of such an inclusive definition, a graphic image of a person is indeed personal information and that legal

---

95 S 16 of the Cybercrimes Act.

96 Naidoo "Hazel Comes Clean on Dirty Laundry and Apologises to Prince Kaybee" (7 May 2021) *The South African* https://www.thesouthafrican.com/lifestyle/celeb-news/prince-kaybee-cheating-zola-who-is-hazel-eurica-latest/ (accessed 2021-01-13).

97 Bond "Understanding Revenge Pornography: A National Survey of Police Officers and Staff in England and Wales" 2021 36(5–6) *Journal of Interpersonal Violence* 2166–2181 doi:10.1177/0886260518760011.

98 Musoni "The Criminalisation of 'Revenge Porn' in South Africa" 2019 *Obiter* 62.

99 *Ibid.*

100 Musoni 2019 *Obiter* 71.

101 S 1 of POPIA.

consequences may result for third parties who process such images in accordance with the definition for "processing". It is therefore important to highlight that the definition of processing in POPIA is wide enough to include further dissemination or sharing:

> "Processing means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including – (*a*) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (*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."[102]

Section 18 of the Act creates various alternatives for when evidence presented in criminal proceedings does not prove the commission of the offence charged, but rather proves a contravention of another section of the Act. Accordingly, an accused may nevertheless be found guilty if an alternative offence is proved. By inserting this provision, the legislature seems to seek to ensure that substance takes precedence over form in criminal proceedings. For example, the right to a fair trial may be a constitutional right sought to be exercised by an accused person, who may raise possibly warranted technicalities.[103] However, the principle of substance over form is observed by the South African legal system as the court in *Van der Walt v S*[104] held:

> "[A]n accused is not at liberty to demand the most favourable possible treatment under the guise of the fair trial right. A court's assessment of fairness requires a substance over form approach. The State correctly submits that the question is accordingly whether the Regional Magistrate committed irregularities or deviated from the rules of procedure aimed at a fair trial, and if so, whether they were of the kind to render the trial unfair."[105]

3 4 Sentencing

Section 19 of the Act is contained in Part V of Chapter 2 and deals with sentencing. This provision particularly sets out the appropriate sentences to be imposed by the courts in the event that a person is found guilty of contravening the provisions of the Act. Section 19(1) provides that where a person is found guilty of contravening sections 2(1) or (2), 3(3) or 7(2), such a person is liable on conviction to a fine or to imprisonment for a period not exceeding five years, or to both a fine and such imprisonment.

Section 19(2) provides that where a person is found guilty of contravening sections 3(1) or (2), 4(1), 5(1), 6(1) or 7(1), such a person is liable on conviction to a fine or to imprisonment for a period not exceeding 10 years or to both a fine and such imprisonment. Section 19(3) provides that where a

---

[102] *Ibid*.

[103] S 34 of the Constitution provides: "Everyone has the right to have any dispute that can be resolved by the application of law decided in a fair public hearing before a court or, where appropriate, another independent and impartial tribunal or forum."

[104] *Van der Walt v S* [2020] ZACC 19; 2020 (2) SACR 371 (CC); 2020 (11) BCLR 1337 (CC).

[105] *Van der Walt v S supra* par 23.

person is found guilty of contravening section 11(1), such a person is liable on conviction to a fine or to imprisonment for a period not exceeding 15 years or to both a fine and such imprisonment. Section 19(4) provides that where the court convicts a person of an offence in terms of sections 8, 9(1) or (2), 10 or 11(2), some limited discretion is afforded where a penalty is not prescribed in respect of that offence by any other law.

The courts are therefore empowered to impose a sentence as provided for in section 276 of the Criminal Procedure Act,[106] as deemed appropriate by the court, provided it is within that court's penal jurisdiction. Section 19(5) provides that where a court imposes any sentence in terms of this section, or where a person is convicted of the offence of theft that was committed or facilitated by electronic means, it must consider certain factors to be aggravating factors.

The list of factors to be considered include that the offence was committed by electronic means; the extent of the prejudice and loss suffered by the complainant or any other person as a result of the commission of the offence; the extent to which the person gained financially, or received any favour, benefit, reward, compensation or any other advantage from the commission of the offence; or that the offence was committed in concert with one or more persons.[107] These factors are discussed in further detail by Watney, where the ambit of receiving favours, benefits, reward and compensation are investigated further. It is important to have regard to Watney's analysis in that she points out the different ways in which more than one person may act in concert with one another to commit offences in terms of the Act.[108]

Section 19(6)(*a*) makes direct imprisonment (with or without a fine) a mandatory sentence where a person is convicted of any offence provided for in sections 2(1) or (2), 3(1), 5(1), 6(1), 7(1), 8, 9(1) or (2), 10 or 11(1) or (2),

---

[106] 51 of 1977. S 276 is titled "Nature of punishments" and provides: "(1) Subject to the provisions of this Act and any other law and of the common law, the following sentences may be passed upon a person convicted of an offence, namely … – (*b*) imprisonment, including imprisonment for life or imprisonment for an indefinite period as referred to in section 286B (1); (*c*) periodical imprisonment; (*d*) declaration as an habitual criminal; (*e*) committal to any institution established by law; (*f*) a fine; … (*h*) correctional supervision; (*i*) imprisonment from which such a person may be placed under correctional supervision in the discretion of the Commissioner or a parole board. (2) Save as is otherwise expressly provided by this Act, no provision thereof shall be construed – (*a*) as authorizing any court to impose any sentence other than or any sentence in excess of the sentence which that court may impose in respect of any offence; or (*b*) as derogating from any authority specially conferred upon any court by any law to impose any other punishment or to impose any forfeiture in addition to any other punishment. (3) Notwithstanding anything to the contrary in any law contained, other than the Criminal Law Amendment Act, 1997 (Act 105 of 1997), the provisions of subsection (1) shall not be construed as prohibiting the court – (*a*) from imposing imprisonment together with correctional supervision; or (*b*) from imposing the punishment referred to in subsection (1)(*h*) or (*i*) in respect of any offence, whether under the common law or a statutory provision, irrespective of whether the law in question provides for such or any other punishment: Provided that any punishment contemplated in this paragraph may not be imposed in any case where the court is obliged to impose a sentence contemplated in section 51 (1) or (2), read with section 52, of the Criminal Law Amendment Act, 1997."

[107] S 19(5)(*a*)–(*d*) of the Cybercrimes Act.

[108] Papadopoulos and Snail *Cyberlaw @ SA IV* ch 13 487.

if the offence was committed by the person (or with the collusion or assistance of another person) who as part of their duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system belonging to another person in respect of which the offence in question was committed.

This is a strict rule imposed by the Act on the court. However, it is trite that there are often exceptions to legal rules.[109] The statutory rule applies strictly, save for instances where substantial and compelling circumstances justify the imposition of another sentence.

Section 19(7) provides that where a person contravenes sections 14, 15 or 16 of the Act, such a person is liable on conviction to a fine or to imprisonment for a period not exceeding three years or to both a fine and such imprisonment.

3 5 Protection of complainant from harmful effects of malicious communications

Section 20(1) provides that a complainant who lays a charge with the South African Police Service (SAPS) that an offence contemplated in section 14, 15 or 16 has allegedly been committed against them may, on an *ex parte* basis, apply to a magistrates' court for a protection order pending the finalisation of the criminal proceedings. It is worth noting that the blanket penalty provisions contained in ECTA simply provided for liability of a fine or imprisonment for periods not exceeding twelve months or five years for the various offences set out therein.[110] The new specifically created sentences signify a shift from the ECTA regime; the Cybercrimes Act provides better protection in that sentences are specific and tailored for the various offences established in the Act.

The purpose of an application in terms of section 20(1) of the Cybercrimes Act is to curtail or prohibit any person from disclosing, or further disclosing the data message to which the charge relates. Alternatively, it may be to order an electronic communications service provider, whose electronic communications service is used to host or disclose the data message relating to the charge, to remove or disable access to the data message.

Section 20(2) provides that in determining such an application, the court *must* consider any additional evidence it deems fit, including oral evidence or evidence by affidavit, which must form part of the record of the proceedings. Section 20(3) provides that if the court determines that there is *prima facie* evidence or are reasonable grounds to believe that an offence referred to in section 14, 15 or 16 has indeed been committed against the applicant, the court may grant the order, subject to such conditions as the court may deem

[109] *See S v Coetzee* [1997] ZACC 2.

[110] S 89 of ECTA: "(1) A person convicted of an offence referred to in section […] 86(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months; (2) A person convicted of an offence referred to in section 86(4) or (5) … is liable to a fine or imprisonment for a period not exceeding five years.

fit. A limited form of discretion is therefore afforded to the court in this context and each case will be tried on its own merits.

Section 21 of the Act is discussed in detail by Watney. The section makes provision that where an application for a protection order is made in terms of section 20(1) and the court is satisfied in terms of section 20(3) that a protection order must be issued and the particulars of the person referred to in section 20(1)(*a*), who discloses the data message, or the electronic communications service provider referred to in section 20(1)(*b*), whose service is used to host or where it is used to disclose the data message, is unknown, the court is entitled to adjourn proceedings on conditions it deems appropriate. The purpose of the adjournment is for the court to order an electronic communications service provider to file an affidavit in which the latter reveals personal information including but not limited to the identity number, name, surname and address associated with the origin of a particular data message.[111]

Other orders that may be made by the courts include those envisaged in section 22 of the Act. These relate to sections 14, 15 and 16. This provision holds that whenever a person is convicted of an offence in terms of the latter sections, but there is evidence that such a person is engaged in harassment as defined in the Harassment Act,[112] the trial court may issue a protection order against such a person. Section 23 specifically provides that any person or electronic communications service provider that is convicted of an offence in terms of sections 20(9) or (10), 21(7) or 22(4) or (8), such a person is liable on conviction to a fine or imprisonment for a period not exceeding two years or to both a fine and such imprisonment.

3 6 Additional provisions in the Cybercrimes Act

3 6 1 Powers to investigate, search, access or seize

Section 25 of the Cybercrimes Act provides pertinent definitions of terms such as “access”, “investigator” and “seize”. Section 26 provides for the issue of standard operating procedures and points out the different personnel within government that are responsible for the consultation process. These include the Minister in consultation with the National Commissioner, the National Head of the Directorate, the National Director of Public Prosecutions and the cabinet member responsible for the administration of justice. Section 26 sets out the standard operating procedures which points out the different personnel within government that are responsible for the consultation process including the Minister in consultation with the National Commissioner, the National Head of the Directorate, the National Director of Public Prosecutions and the Cabinet member responsible for the administration of justice. These SOPs do not only affect the Police, it affects the investigator appointed in terms of Cybercrimes Act, any person authorised in terms of any other law to

111 Papadopoulos and Snail *Cyberlaw @ SA IV* ch 13 485.
112 17 of 2011.

investigate any offence, to follow the same SOPs.[113] It is unclear if the other entities are aware that they are supposed to make comments on the SOPs.[114] With regards to the computer evidence, the sections dealing with, is still section 15 of the ECT Act, and the validity and weight of the evidence is still under this section. Section 27 provides that the Criminal Procedure Act (CPA)[115] applies to Chapter 4, insofar as it is not inconsistent with the Cybercrimes Act.[116]

Section 28 confers police officials with the authority to search for, gain access to, or seize certain articles. Section 29 delineates the types of article that may be subject to a warrant in terms of section 28.[117] Section 30 provides that application for such a warrant may be made orally.[118] Section 31 confers authority to exercise the powers in section 28 without a warrant, but with the consent of a person who has authority to give such consent.[119] Section 32 confers authority on police officials to exercise powers set out in section 28 without a warrant.[120] Section 33 confers authority upon a police officer to conduct an arrest without a warrant against any person who commits an offence in terms of Parts I or II of Chapter 2 of the Act.[121]

Section 34 makes it obligatory for electronic communications service providers, financial institutions, or persons who are in control of information, objects or facilities, to assist a police official by providing technical assistance and any other necessary assistance in the investigation process concerning a cybercrime suspect.[122] Failure to comply with this provision is an offence.[123] Section 35 makes it an offence to obstruct or hinder a police official exercising powers in terms of sections 28 and 29 of the Act.[124] Police officials are also empowered to use force.[125]

Section 36 requires police officials to exercise their powers decently and without infringing upon other persons' rights. It is important to note that a search upon a female person may only be conducted by a female official; but there is no requirement in the provision for a male person to be searched only by a male official.[126] Section 37 sets out that an offence is committed where a police official exercises section 28 powers wrongfully.[127]

---

113 Esselaar (*Sub*) "Standard Operating Procedure of Cybercrimes Act" http://www.esselaar.co.za/legal-articles/sub-standard-operating-procedures-cybercrimes-act (accessed 2022-07-31) 1.

114 *Ibid*.

115 51 of 1977.

116 S 27(1) of the Cybercrimes Act.

117 S 28(2) of the Cybercrimes Act.

118 S 30(1) of the Cybercrimes Act.

119 S 31(1) of the Cybercrimes Act.

120 S 32(1) of the Cybercrimes Act.

121 S 33(1) of the Cybercrimes Act.

122 S 34(1) of the Cybercrimes Act.

123 S 34(2) of the Cybercrimes Act.

124 S 35(1) of the Cybercrimes Act.

125 S 35(2) of the Cybercrimes Act.

126 S 36(2) of the Cybercrimes Act.

127 S 37(1) of the Cybercrimes Act.

Section 38 creates an offence where any person provides false information under oath in relation to the provisions set out in Chapter 4.[128] Section 39 provides that it is unlawful to disclose information gathered during an investigation, unless certain exceptions apply.[129] Section 40 sets out what constitutes lawful interception of indirect communication. Section 41 empowers a designated police official to issue a preservation of data direction against any electronic communications service provider referred to in section 40(3) or a financial institution that is in possession of, receives, or is in control of, certain data.[130]

Section 41 provides that an expedited preservation of data direction may be issued by a police official where certain requirements are met.[131] Section 42 accordingly confers powers upon magistrates or judges to issue a preservation of evidence direction.[132] Section 43 of the Act provides that an application for such a direction may be made orally.[133] Section 44 provides for the disclosure of data in terms of section 29(1).[134] Section 45 provides that a police official may, without authorisation, obtain and use publicly available data from a person who is in possession of it.[135]

3 6 2 Mutual assistance

Section 46 of the Act provides that sections 48 to 51 apply in addition to the International Co-operation in Criminal Matters Act.[136] Section 47 provides that the National Commissioner or the National Head of the Directorate may provide information to a foreign law enforcement agency.[137] Section 48 relates to foreign requests for assistance and cooperation. It provides that a designated point of contact may lawfully give certain information requests to a foreign authority, court or tribunal.[138]

Section 49 makes it obligatory for an electronic communications service provider or financial institution to comply with an order of a designated judge in terms of section 48(6).[139] Section 50 provides that the National Director of Public Prosecutions (NDPP) must inform the designated judge or applicable authority in a foreign state of the outcome of a request for assistance and cooperation.[140] Section 51 provides for the issuing of a direction requesting assistance from a foreign state.[141]

---

128 S 38(1) of the Cybercrimes Act.
129 S 39(1) of the Cybercrimes Act.
130 S 40(1) and (3) of the Cybercrimes Act.
131 S 41(1) of the Cybercrimes Act.
132 S 42(1) of the Cybercrimes Act.
133 S 43(1) of the Cybercrimes Act.
134 S 44(1) of the Cybercrimes Act.
135 S 45(*a*)–(*b*) the Cybercrimes Act.
136 75 of 1996.
137 S 47(1) of the Cybercrimes Act.
138 S 48(1) of the Cybercrimes Act.
139 S 49(1) of the Cybercrimes Act.
140 S 50(1) of the Cybercrimes Act.
141 S 51(1) of the Cybercrimes Act.

3 6 3 Establishment of designated point of contact

Section 52 is contained in Chapter 6 of the Act. This section obliges the National Commissioner to establish or designate an office within existing structures of SAPS to be known as the designated point of contact for South Africa.[142] The designated point of contact's mandate in terms of the Act is to ensure the provision of assistance for the purpose of proceedings or investigations regarding the commission of offences in terms of Parts I and II of Chapter 2 or other offences.[143]

3 6 4 Evidence

Section 53 provides for the adducing of evidence by way of affidavit in relation to the interpretation of data; the design or functioning of data, a computer program, a computer data storage medium or a computer system; computer science; electronic communications networks and technology; software engineering; or computer programming. This section makes expertise a requirement for such evidence,[144] and creates an offence where false information is produced as evidence.[145]

3 6 5 Reporting obligations and capacity building

Sections 54 to 56 are contained in Chapter 8 of the Cybercrimes Act. Section 54 provides that an electronic communications service provider must, within 72 hours of having become aware thereof, report an offence committed in terms of Part I of Chapter 2 to SAPS.[146] It is important that a failure to report in terms of this provision makes such a party guilty of an offence and liable on conviction to a fine not exceeding R50 000.[147]

Section 55 provides that the cabinet minister responsible for policing must establish and maintain sufficient human and operational capacity to detect, prevent and investigate cybercrimes,[148] ensure that police officials have the requisite training,[149] and develop accredited training programmes for SAPS members to achieve this purpose in cooperation with institutions of higher learning.[150] Section 56 of the Act provides that the NDPP must keep statistics of prosecutions relating to cybercrimes.[151] The Cybercrimes Act, in regulating the entire terrain of cybercrime as it is perceived currently, offers greater legal protection for victims of cybercrimes, guidance to law enforcement agencies and legal certainty for the courts. The creation of

142 S 52(1) of the Cybercrimes Act.
143 S 52(5) of the Cybercrimes Act.
144 S 53(1) of the Cybercrimes Act.
145 S 53(2) of the Cybercrimes Act.
146 S 54(1) of the Cybercrimes Act.
147 S 54(3) of the Cybercrimes Act.
148 S 55(1)(*a*) of the Cybercrimes Act.
149 S 55(1)(*b*) of the Cybercrimes Act.
150 S 55(1)(*c*) of the Cybercrimes Act.
151 S 56(1) and (2) of the Cybercrimes Act.

specific offences as well as sentences is a move towards more efficient cybercrime regulation than was previously afforded in terms of the common law and ECTA.

In the discussion that follows, the terrain of data protection and privacy is explored from both a constitutional and statutory perspective. This article discusses both data protection and cybercrime because there are some areas of common ground between these two separate areas of the law. It is therefore submitted that discussing them together is useful for understanding the risks associated with the use of computers, the processing of data and the legal remedies afforded to persons who find themselves in need of legal protection.

4 DATA PROTECTION IN TERMS OF THE CONSTITUTION, THE COMMON LAW AND LEGISLATION

Data protection laws in the Republic of South Africa are first and foremost rooted in the Constitution,[152] which is the supreme law of the land. Although it is true and factually correct that data protection laws in the Republic have their antecedents in foreign and international legal dispensations,[153] the submissions made here are limited to the South African legal position as it has matured over the years. The Constitution protects the right to privacy in terms of section 14, which provides:

> "Everyone has the right to privacy, which includes the right not to have–
> (a) their person or home searched;
> (b) their property searched;
> (c) their possessions seized; or
> (d) the privacy of their communications infringed."

The status enjoyed by the Constitution in South Africa is high; it is the legal instrument that has a higher status than any other legislation enacted by Parliament. This position is best described in a pronouncement of the court in the case of *Doctors for Life International v Speaker of the National Assembly*,[154] where the court held:

> "But under our constitutional democracy, the Constitution is the supreme law. It is binding on all branches of government and no less on Parliament. When it exercises its legislative authority, Parliament 'must act in accordance with, and within the limits of, the Constitution', and the supremacy of the Constitution requires that 'the obligations imposed by it must be fulfilled'. Courts are required by the Constitution 'to ensure that all branches of government act within the law' and fulfil their constitutional obligations."

For practical purposes within the context of data protection, section 14 serves the purpose of prohibiting any unlawful processing of personal information. The definition of "processing" in POPIA is wide enough to

---

152 Constitution of the Republic of South Africa, 1996.

153 Van der Merwe *Information and Communications Technology Law* (2016).

154 [2006] ZACC 11; 2006 (6) SA 416 (CC) par 68–69; 2006 (12) BCLR 1399 (CC). This case was also cited in the landmark case of *Glenister v President of the Republic of South Africa* [2008] ZACC 19; 2009 (1) SA 287 (CC); 2009 (2) BCLR 136 (CC).

encompass a number of actions that may be conducted with personal information. This definition entails a non-exhaustive list of actions as follows:

> "(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." [155]

An interpretation of the constitutional right to privacy was given in the case of *Mistry v Interim National Medical and Dental Council.*[156] The court considered searches and communications made in terms of the Medicines Act[157] and the Medical Act.[158] Substantial remarks regarding the appropriateness of an investigator's infringement upon the right to information privacy were made. In making its findings, the court had to consider whether the aforementioned medical acts provided sufficient basis for a limitation on the right to privacy.[159] The court did not deem it absolutely necessary to perform a strict balancing act between the right to privacy in terms of section 13 of the Interim Constitution in view of the aforementioned medical acts and the limitation clause (section 33) of the Interim Constitution. The following remarks were, however, made by the court:

> "The right to informational privacy is covered by the broad protection of privacy guaranteed by section 13. The second is that Mr Enslin was at all material times fulfilling state functions and, as such, obliged to respect the provisions of the Bill of Rights, including section 13.72. The third assumption – in line with the finding of McLaren J – is that Mr Enslin breached section 41(A)(9)(*a*) of the Medical Act in informing Mr Coote of the fact of the complaint against the applicant and of the proposed investigation, and also in communicating with Mr Coote during the inspection."[160]

4 1 An overview of POPIA's most salient provisions

POPIA contains specific principles or guidelines for the processing of personal information. These are formally known in the Act as the "conditions" for the lawful processing of personal information.[161] The eight conditions set out between sections 8 and 25 of the Act are accountability;[162] processing limitation;[163] purpose specification;[164] further processing limitation;[165]

155 S 1 of POPIA.

156 1998 (4) SA 1127 (CC).

157 Medicines and Related Substances Act 101 of 1965.

158 Medical, Dental and Supplementary Health Service Professions Act 56 of 1974.

159 Constitution of the Republic of South Africa Act 200 of 1993. Section 13 of the Interim Constitution provided that, "Every person shall have the right to his or her personal privacy, which shall include the right not to be subject to searches of his or her person, home or property, the seizure of private possessions or the violation of private communications." The court considered whether the limitation clause (Section 33) was applicable in the circumstances.

160 *Mistry v Interim National Medical and Dental Council supra* par 48.

161 De Stadler and Esselaar *Guide to Protection of Personal Information Act* (2020) 1.

162 S 8 of POPIA.

163 Ss 9–12 of POPIA.

information quality;[166] openness;[167] security safeguards;[168] and data subject participation.[169] Burns and Burger-Smidt characterise the conditions as minimum requirements for the processing of personal information, and they point out that legal instruments from the European Union have informed the distillation of these conditions.[170]

Included in these conditions, which are explained later in this article, is the positive duty on responsible parties to disclose breaches in the proper processing of information. POPIA sets out the complaints procedure to be instituted with the Information Regulator, as well as the civil remedies available to data subjects if their right to privacy is infringed.[171]

In the context of POPIA, the route to be followed for the enforcement of rights is: the lodgement of complaints; decisions by the Information Regulator whether to institute pre-investigation or conciliatory proceedings or full investigation; the settlement of complaints at an early stage in the proceedings; the issue and execution of warrants of entry, search and seizure; the assessment by the Information Regulator regarding the lawfulness or otherwise of the processing procedure; decisions on how to deal with information notices; referrals to an enforcement committee; enforcement notices lodging appeals in the High Court; and reliance on civil remedies.[172]

It is worth noting that the ambit of the right to privacy as expressed in the Constitution provides that, "[e]veryone has the right to privacy, which includes the right not to have … their property searched",[173] and not to have "their possessions seized."[174] Musoni investigates cyber search and seizure in light of both the Cybercrimes Act (in its form as a Bill at the time of writing) and POPIA. She notes that a search often entails a serious encroachment upon an individual's right to privacy.[175] In her discussion, Musoni draws from common-law judicial precedent to investigate whether the mechanism entitling police officials to use warrants to conduct a search and seizure in terms of the Act is not so wide as arbitrarily to infringe upon the right to privacy.[176]

Musoni firstly draws on the legal position as adopted in *Minister of Safety and Security v Van der Merwe*,[177] where the court held that in order for a

164 Ss 13 and 14 of POPIA.
165 S 15 of POPIA.
166 S 16 of POPIA.
167 Ss 16 and 17 of POPIA.
168 Ss 19–22 of POPIA.
169 Ss 23–25 of POPIA.
170 Burns and Burger-Smidt *A Commentary on the Protection of Personal Information Act* (2018) 43.
171 De Stadler and Esselaar *Guide to Protection of Personal Information Act* 1.
172 Burns and Burger-Smidt *A Commentary on the Protection of Personal Information Act* 219.
173 S 14(*b*) of the Constitution.
174 S 14(*c*) of the Constitution.
175 Musoni "Is Cyber Search and Seizure Under the Cybercrimes and Cybersecurity Bill Consistent With the Protection of Personal Information Act?" 2016 *Obiter* 690.
176 *Ibid.*
177 2011 (2) SACR 301 (CC) par 55–56.

search warrant to be valid, it must: state the statutory provision(s) in terms of which it is issued; identify the searcher; clearly mention the authority it confers upon the searcher; describe the person, container or premises to be searched; describe the article to be searched or seized with sufficient particularity; specify the offence that triggered the criminal investigation; and specify the names of the suspected offenders. Musoni offers a critique of the Cybercrimes Act in that it remains wide, and thus permits police officials to rifle arbitrarily through an individual's emails, social networking profiles, data messages, computer files and various other forms of data that may contain personal information but may not be relevant for the purposes of the criminal investigation.[178] Such a critique demonstrates the need for coherence between data protection and cybercrime legislation.

POPIA was signed into law on 19 November 2013 and its provisions began to enjoy full application from 1 July 2021, when responsible parties had to ensure compliance with the Act, failing which legal consequences would follow as the Information Regulator had been conferred with full powers to operate as a data protection authority.[179] A critical characteristic of POPIA is that it is an enabling Act, rather than an inhibiting one. This is so in that the conditions set out in the Act are what they purport to be – that is, conditions. They are for all intents and purposes to be seen as guiding principles within the ambit of which lawful processing of personal information can take place.

This is to say that POPIA does not set out to prohibit the processing of personal information, but rather to ensure that such processing is lawful, necessary and not excessive, among other limitations.[180] It is for this reason that the conditions for lawful processing of personal information are set out and discussed further in this article. From a practical perspective, it is important to note that the provisions of the Act have not found specific interpretation by the courts, but there has been some discourse emanating from the case of *Black Sash Trust v Minister of Social Development,*[181] where the court held:

> "SASSA is under a duty to ensure that the payment method it determines … contains adequate safeguards to ensure that personal data obtained in the payment process remains private and may not be used for any purpose other than payment of the grants or any other purpose sanctioned by the Minister … precludes a contracting party from inviting beneficiaries to 'opt in' to the sharing of confidential information for the marketing of goods and services."

---

178 *Ibid*.

179 Commencement dates for POPIA https://www.popiact-compliance.co.za/popia-information (accessed 2021-07-12): "Sections 2 to 38; sections 55 to 109; section 111; and section 114 (1), (2) and (3) shall commence on 1 July 2020. Sections 110 and 114(4) shall commence on 30 June 2021. Sections 2 to 38; sections 55 to 109; section 111; and section 114 (1), (2) and (3). Sections 110 and 114(4) shall commence on 30 June 2021. Please see the official Press Release from the Presidency of the Republic of South Africa "Commencement of certain sections of the Protection of Personal Information Act, 2013" (22 June 2020) http://www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013 (accessed 2021-07-12).

180 Ss 8–13 of POPIA.

181 *Black Sash Trust v Minister of Social Development supra*.

4 2 The conditions for the lawful processing of personal information

The conditions must be observed and adhered to, unless specific exemptions apply in terms of the Act.[182] In the discussion that follows, a concise summary of the conditions is made. Condition 1 is the *accountability* condition, the meaning of which is self-evident.[183] Responsible parties are obliged to be accountable to data subjects in their exercise of the function of processing their personal information.[184] It is incumbent upon both responsible parties to ensure that obligations imposed by data privacy laws are observed for the benefit of the data subject, and that where obligations are placed by POPIA *vis-à-vis* the Information Regulator or any relevant party, such obligations are honoured and observed.

Condition 2 is the *processing limitation* condition,[185] where in order for processing to be lawful, responsible parties should deliberate and be cognisant of the reason that such personal information is processed, the type of personal information involved, and the persons from whom it is collected. Lawfulness of processing is a subset of this condition, which prescribes that the processing of personal information must not be done for an unlawful purpose.[186]

Minimality is another subset of the processing limitation condition; it places a bar on the processing of personal information where the purpose of processing is inadequate, irrelevant and excessive.[187] Consent, justification and objection form the third subset of the processing limitation condition. This subset places importance upon the involvement of a data subject in the processing of their personal information.[188] In this respect, it is important to note what consent is and is not. The Act specifically defines consent in such a manner that it is only valid when it is voluntary, specific and informed.[189]

It is incumbent upon a responsible party to ensure that any exceptions or deviations from the consent condition are made in accordance with the ambit of the Act's provisions – whether these relate to direct marketing or some other ground. Direct collection from data subjects is the fourth and final subset of the processing limitation condition, which imposes a strict requirement for direct collection. However, as with most rules, there are

---

182 Thaldar "Protecting Personal Information in Research: Is a Code of Conduct the Solution?" 2021 117 *South African Journal of Science* 3.

183 S 8 of POPIA: "The responsible party must ensure that the conditions set out in this Chapter, 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 itself."

184 S 1 defines a "responsible party" as follows: "The responsible party is the 'public or private body or any other person, which alone or in conjunction with others, determines the purpose of and means for processing personal information.'"

185 Ss 9–12 of POPIA.

186 S 9 of POPIA: "Personal information must be processed – (*a*) lawfully; and (*b*) in a reasonable manner that does not infringe the privacy of the data subject."

187 S 10 of POPIA: "Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive."

188 S 11 of POPIA.

189 S 1 of POPIA.

exceptions.[190] It may be impractical for example to meet such a condition where the personal information is contained in a public record; or if it was made public by the data subject.

Condition 3 is *purpose specification*. This condition prescribes that personal information must be collected for a purpose that is specific, explicitly defined and lawful.[191] Accordingly, the first subset of this condition is collection for a specific purpose. In the event that this condition is not observed, responsible parties may expose themselves to remedies that data subjects pursue, or that are imposed by the Information Regulator or civil remedies instituted in alternative forums such as the courts.

The second subset of this condition relates to the retention and restriction of records.[192] This condition provides that records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed. Exceptions to this condition entail further processing for statistical, historical and research purposes, provided there are proper safeguards in place to protect the personal information.[193]

Condition 4 is the *further processing* limitation. Further processing of personal information is unlawful if it is no longer compatible with the original purpose of collection. A determination of compatibility is efficiently dealt with where the relationship between the responsible party and the data subjects, or where applicable between a responsible party and an operator, clearly sets out a limitation on further processing.[194]

Condition 5 is *information quality*, which makes it obligatory for responsible parties to take reasonably practicable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary.[195] It is important to note that the purpose of processing such information is the benchmark to justify such processing.[196] The importance of such a condition is seen in instances where a contractual dispute arises between a data subject and a responsible party such as a financial institution, where the latter institutes legal proceedings on the basis of personal information collected and sets out a domicile address.

Condition 6 is *openness*, which makes it obligatory for responsible parties to maintain information manuals of their processing activities and accordingly to make crucial information available to data subjects when

190 S 12 of POPIA.

191 S 13 of POPIA: "(1*)* Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party; (2) Steps must be taken in accordance with section 18(1) to ensure that the data subject is aware of the purpose of the collection of the information unless the provisions of section 18(4) are applicable."

192 S 14 of POPIA.

193 S 14(2)–(8) of POPIA.

194 S 15 of POPIA.

195 S 16(1) of POPIA.

196 S 16(2) of POPIA.

called upon to do so.[197] It is incumbent on a responsible party to inform a data subject when personal information is collected, the purpose of its collection, the name and address of the responsible party, whether it is mandatory/necessary or not to provide the information, consequences for any failure to provide information, whether the collection is done in terms of a legal obligation, and whether the responsible party intends to transfer the information outside Republic of South Africa and any other relevant information.[198]

De Stadler and Esselaar expand on the content of the openness condition, first by highlighting that this condition requires that data subjects be informed when personal information is collected.[199] Secondly, they point out that the purpose of collection in terms of section 13 must be communicated to the data subject *before* the personal information is collected.[200] Burns and Burger-Smidt take the discussion further by bringing the principles of openness and transparency within the purview of the Constitution.[201] They state:

> "[T]he requirements of openness and transparency are well-known principles of a democratic system of government. Decisions which are shrouded in secrecy lead to suspicion and distrust."[202]

These sentiments are echoed in this article to buttress the view that openness is not only an important condition for lawful processing in terms of POPIA, but also a constitutional principle that must be observed in doing so. There are instances where the right to privacy must be weighed up against the right of access to information. In such instances, the principle of openness and transparency is tested. The importance of this principle has been demonstrated in the case of *My Vote Counts NPC v Minister of Justice and Correctional Services*,[203] where the court stated the test for lawful access to and exchange of an individual's personal information.

Condition 7 is *security safeguards*¸ which places an obligation upon responsible parties to apply appropriate, reasonable, technical and organisational steps in terms of section 19 of POPIA. The Act is instructive in the sense that it first points out that these steps or measures must be taken in order to prevent loss of, damage to or unauthorised destruction of personal information, and unlawful access to or processing of personal information.[204]

---

197 S 17 of POPIA, read together with s 14 or s 51 of the Promotion of Access to Information Act 2 of 2000.

198 S 18 of POPIA.

199 De Stadler and Esselaar *A Guide to the Protection of Personal Information Act* 18.

200 De Stadler and Esselaar *A Guide to the Protection of Personal Information Act* 19.

201 Burns and Burger-Smidt *A Commentary on the Protection of Personal Information Act* 66.

202 S 1 of the Constitution provides: "The Republic of South Africa is one, sovereign, democratic state founded on the following values: (*a*) Human dignity, the achievement of equality and the advancement of human rights and freedoms; (*b*) Non-racialism and non-sexism; (*c*) Supremacy of the constitution and the rule of law; (d) Universal adult suffrage, a national common voters roll, regular elections and a multi-party system of democratic government, to ensure accountability, responsiveness and openness."

203 *My Vote Counts NPC v Minister of Justice and Correctional Services* [2018] ZACC 17.

204 S 19(1)(*a*) and (*b*) of ¸POPIA.

This condition not only places legal obligations on responsible parties, but on operators as well.[205] Secondly, the Act maps out a further purpose for taking such measures.[206] It is important to note that this is the measure aimed at preventing data breaches and in this context, the convergence of cybercrime and data protection laws is most evident. The best example of this is the obligation upon responsible parties and operators to notify data subjects and the Information Regulator if the security of personal information is compromised.[207]

Condition 8, the final condition, is *data subject participation*, which protects the constitutional right of access to personal information and the right to the maintenance of correct personal information as being inherent in the right to privacy.[208] This ensures that responsible parties maintain correct information in addition to Condition 5,[209] and provides guidance on the manner of accessing such information.

This condition provides that where access to information requests are made in terms of sections 18 and 53 of PAIA, this ought to be done in compliance with section 23 of POPIA.[210] In terms of the right of access to information, data subjects are entitled to know that their personal information is held by responsible parties. Data subjects are also entitled to call upon responsible parties to produce proof of consent conferring upon them the authority to process their (the data subjects') personal information.

4 3 Offences, penalties, administrative fines and enforcement of POPIA

POPIA sets out offences,[211] penalties,[212] and administrative fines where infringements to its provisions occur.[213] The specific offences set out in the Act are "obstruction of Regulator", "breach of confidentiality", "failure to comply with enforcement notices", "failure to comply with information notices", "offences committed by witnesses", and "unlawful acts by responsible parties in connection with account number".[214]

Section 107 of the Act provides that any person convicted of an offence contained in sections 100, 103(1), 104(2), 105(1), or 106(1), (3) or (4) is

[205] Ss 20 and 21 of POPIA.

[206] S 2 of POPIA: "In order to give effect to subsection (1), the responsible party must take reasonable measures to – (*a*) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; (*b*) establish and maintain appropriate safeguards against the risks identified; (*c*) regularly verify that the safeguards are effectively implemented; and (*d*) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards."

[207] S 22 of POPIA.

[208] S 23 of POPIA.

[209] S 24 of POPIA.

[210] S 25 of POPIA.

[211] Ss 100–106 of POPIA.

[212] Ss 107 and 108 of POPIA.

[213] S 109 of POPIA.

[214] S 100 of POPIA.

liable to a fine or imprisonment not exceeding 10 years.[215] Where there is an offence committed in terms of sections 59, 101, 102, 103(2) or 104(1), the Act provides for a fine or imprisonment for a period not exceeding 12 months.[216] It is important to note that in terms of these provisions, the court is empowered to mete out a sentence that constitutes both a fine and imprisonment.

POPIA confers powers upon the Information Regulator to deliver by hand to a responsible party who commits an offence specified in terms of the Act an infringement notice.[217] Such a notice must specify the name and address of the infringer,[218] the particulars of the alleged offence,[219] and the amount of the administrative fine payable by the infringer.[220] It is important to note that POPIA places a cap on the fine that may be imposed upon an infringer. The maximum amount payable as a fine, subject to subsection (10), may not exceed R10 000 000.00 per incident. The factors to be considered by the Regulator when determining an appropriate fine are set out in section 109(3) of POPIA.

POPIA creates an offence in the event that account information is passed onto a third party without the requisite authority from a data subject. POPIA is data protection legislation that regulates the lawful processing of personal information; in so doing, it places a duty upon responsible parties to safeguard such information by having technical and organisational measures in place to achieve this. This duty also entails cybersecurity imperatives in the form of responsible parties being in a position to identify internal or external security threats and vulnerabilities. The Cybercrime Act contains substantive and procedural measures to curtail cybercriminality, even in the context of personal information protection and the protection of incorporeal things. The convergence of laws on data protection and cybercrime is discussed next.

5 THE CONVERGENCE OF CURRENT LAWS ON CYBERCRIME AND DATA PROTECTION

It is also important to note that the convergence argument advanced in this article becomes clear when consideration is given to the fact that criminal consequences remain within the enforcement authority of the South African Police Service, the National Commissioner, the NDPP, the cabinet minister responsible for policing and other law enforcement functionaries. It is also important to note that POPIA provides an election that may be made by a responsible party to be tried in court for having committed an alleged offence.[221] Consideration may be given to section 109(6), which provides:

[215] S 107(1) of POPIA.
[216] S 107(2) of POPIA.
[217] S 109(1) of POPIA.
[218] S 109(2)(*a*) of POPIA.
[219] S 109(2)(*b*) of POPIA.
[220] S 109(2)(*c*) of POPIA.
[221] S 109(4) of POPIA.

> "[T]he Regulator may not impose an administrative fine contemplated in this section if the responsible party concerned has been charged with an offence in terms of this Act in respect of the same set of facts."

It is clear from the above that a law enforcement agency or another party may lay charges against a responsible party for the commission of an offence in terms of POPIA. In such event, the Regulator is accordingly limited in its powers to administer administrative fines.[222]

It is therefore reiterated that a convergence of cybercrime legislation and data protection legislation becomes evident in such circumstances. It is submitted that the provisions contained in the Cybercrimes Act are quite extensive. The creation of the Regulator provides an extra body that is necessary to curtail the occurrence and perpetuation of cybercrime.

This is especially true when consideration is given to the golden thread in the Cybercrimes Act, which is the imposition of mandatory obligations upon electronic communication service providers and financial institutions to cooperate with police officials. It is submitted that these service providers and financial institutions are in fact responsible parties in terms of POPIA. The available literature, including Watney's extensive discussion on cybercrime law demonstrates that the Cybercrimes Act is important legislation that has built on the common-law position and ECTA, and whose application has a bearing on data protection legislation such as POPIA.

6 CONCLUSION

It is submitted that there is a level of coherence in cybercrime and data protection laws in South Africa. Both the Cybercrimes Act and POPIA deal substantively and procedurally with the legal effects of data security and data vulnerability. Although criticism may be levelled at the length of time it has taken to enact such legislation since cybercrimes began to be a threat in the South Africa cyberspace, the law has not been completely silent; ECTA and the common law have been in place to provide remedies for victims of cybercrimes. Furthermore, the Constitution's protection of the rights to privacy and access to information has to an extent provided a legal basis for persons to take the steps in the courts where necessary.

[222] S 107 of POPIA.