INTERPRETING THE PROVISIONS OF THE CYBERCRIMES ACT 19 OF 2020 IN THE CONTEXT OF CIVIL PROCEDURE: A FUTURE JOURNEY

Nombulelo Queen Mabeka
LLB LLM LLD
Admitted Attorney of the High Court
Senior Lecturer, Department of Jurisprudence
University of South Africa (UNISA)

Fawzia Cassim (In Memory)
BA LLB LLM LLD
Admitted Attorney and Conveyancer of the High Court
Associate Professor, Department of Criminal and Procedural Law
University of South Africa (UNISA)

SUMMARY

It is accepted nowadays that cyberspace is used extensively to commit cybercrimes and cybersecurity offences. Victims of cybercrime can use civil procedure to institute claims for damages. Civil procedure is a branch of law that allows victims of cyberspace crimes to institute claims for damages. This article examines the impact of the Cybercrimes Act 19 of 2020 (Cybercrimes Act) on South African civil procedure. It appears that a contravention of the Cybercrimes Act may result in financial problems for the plaintiff, which then enables the latter to institute a civil claim against the defendants. The authors determine whether contravening the provisions of the Cybercrimes Act gives rise to a cause of action that permits the plaintiff to institute civil proceedings for damages suffered. While the Cybercrimes Act is lauded for its provisions addressing cybercrime, room for improvement is identified. Lastly, the authors conduct a comparative analysis between the provisions of the Cybercrimes Act and the Budapest Convention.

1 INTRODUCTION

Civil procedure is "part of Civil Law", which stems from Justinian's *Corpus Juris Civilis*.[1] Tetley defines "Civil Law" as the legal traditions that come from Roman-Dutch law and which the courts have applied in settling civil disputes.[2] Civil procedure deals with the law relating to procedures applied in civil litigation in our courts. In terms of South African common law, a civil court is vested with jurisdiction (or competence) to hear a matter in respect of monetary claims if a contract was concluded, was to be performed or has been breached within the court's jurisdictional area;[3] or if a delict on which a claim is based was committed within a court's jurisdictional area.[4] The above two grounds are known as *ratione rei gestae,* particularly in the High Court. The magistrates' courts are regarded as "creatures of statute" because their jurisdiction is limited to claims of up to R400 000.[5] This implies that should a civil claim that accrues from a contravention of the stipulations of the Cybercrimes Act be less than R400 000, the plaintiff may refer the claim to a magistrates' court.

Actor sequitur forum rei (a common-law principle that has been applied for decades) is significant in civil procedure.[6] It simply means that the plaintiff follows the defendant because of the doctrine of effectiveness.[7] Thus, the plaintiff must institute civil proceedings in a court that will be able to enforce the judgment. This is the court where the defendant is domiciled,[8] or where the cause of action arises or where the property of the defendant is situated.[9] The *actor sequitur forum rei* principle is significant because when the defendant contravenes provisions of the Cybercrimes Act, the plaintiff who is a victim, must follow the defendant so that the outcome of the court can be enforced.

It is trite law that defamation cases are civil cases that are heard in civil courts. Civil procedure is a branch of law that allows victims of cyberspace crimes to institute claims for damages.[10] Cyberspace is used to commit cybercrimes and cybersecurity offences.[11] The courts dealt with early cyberspace cases in *Le Roux v Dey*[12] and *Manyi v Dlamini*[13] respectively, which then led to the drafting of the Cybercrimes Act, which, *inter alia*,

---

1 Tetley "Mixed Jurisdictions: Common Law (Codified and Uncodified)" 2000 *Louisiana Law Review* 678–738.

2 Tetley 2000 *Louisiana Law Review* 683.

3 This is known as *ratione contractus*.

4 This is known as *ratione delicti commissi*.

5 Theophilopoulos, Van Heerden, Borraine and Rowan *Fundamental Principles of Civil Procedure* 4ed (2020) 53.

6 Theophilopoulos *et al Fundamental Principles of Civil Procedure* 56.

7 *Ibid*.

8 Theophilopoulos *et al Fundamental Principles of Civil Procedure* 59.

9 Theophilopoulos *et al Fundamental Principles of Civil Procedure* 75.

10 Roos and Slabbert "Defamation on Facebook: *Isparta v Richter* 2013 6 SA 529 GP' 2014 17 *Potchefstroom Electronic Law Journal* 2845 and 2861.

11 *Le Roux v Dey* (2011) 3 SA 274 (CC); *Manyi v Dhlamini* 2018 ZAGPPHC 563.

12 *Supra*.

13 *Supra*.

prohibits cyberspace crimes such as unlawful access.[14] Section 16 also criminalises the disclosure of "intimate images" without consent. In the case of *Le Roux v Dey*, the court confirmed that the distribution of intimate pictures suggesting that Dr Dey was in a gay relationship amounted to a cause of action.

The Cybercrimes Act imposes severe penalties in order to send a strong message to perpetrators and to show that the legislature intends to protect victims of cybercrimes. For example, section 23 provides for sanctions such as fines or imprisonment when the Cybercrimes Act is contravened. The Act's stipulations also fetter the right to freedom of expression, which many use as a defence when publishing derogatory statements on social media.[15]

The Cybercrimes Act addresses, *inter alia*, unlawful access,[16] unlawful interception of data,[17] unlawful interference with data,[18] cyber fraud,[19] cyber forgery and uttering[20] and malicious communications.[21]

It is evident that a contravention of the provisions of the Cybercrimes Act, more often than not, causes damages to a victim (or plaintiff). It is for this reason that the authors argue that some provisions should be incorporated into the Cybercrimes Act to allow plaintiffs who suffer damages as a result of an infringement to pursue civil proceedings. The authors also examine the Cybercrimes Act in light of both superior courts and the lower courts by looking at the relevant rules of these courts. Lastly, the authors conduct a brief comparative analysis between the Budapest Convention[22] and relevant stipulations of the Cybercrimes Act to see whether lessons can be gleaned for application in South African civil procedure.

2 DEFINING CYBERCRIMES AND CYBER DEFAMATION

It is important to point out that the Cybercrimes Act does not define cybercrimes. However, the courts and authors offer different definitions. Cybercrime involves the commission of a crime using a computer, a computer network or a networked device.[23] A computer may become the "object" of a crime when theft of the computer hardware or software occurs.[24] It may also become the "subject" of a crime when it is used as an instrument to commit crimes such as fraud, theft, denial of service attacks,

14 S 2 of the Cybercrimes Act.
15 *Manuel v Economic Freedom Fighters* (2019) 5 SA 210 (GJ) par 2.
16 S 2 of the Cybercrimes Act.
17 S 3 of the Cybercrimes Act.
18 S 5 of the Cybercrimes Act.
19 S 8 of the Cybercrimes Act.
20 S 9 of the Cybercrimes Act.
21 Part II of the Cybercrimes Act.
22 Council of Europe *Convention on Cybercrime* CETS 185 (23 November 2001) (Adopted: 23/11/2001; EIF: 01/07/2004).
23 Cassim "Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study" 2009 *PER* 37/360.
24 *Ibid.*

identity theft, cyberbullying or cyber defamation.[25] Thus, a computer may be used in the commission of a crime or be the target.[26] The development of new accessible technologies and the expansion of the Internet have also resulted in new forms of criminal behaviour.[27] The cybercrime problem has now become a global problem, with cybercriminals and hackers exploiting the Internet for monetary gain.

Cyber defamation involves the act of intentionally insulting or defaming another individual or party through a virtual medium.[28] The Internet has facilitated the sharing of ideas and opinions globally. This makes it easier to cause harm through false statements in cyberspace. The law on defamation is said to apply to speech on the Internet.[29] Therefore, people can no longer express their opinions on social networking sites without bearing the consequences. The law of defamation enables the plaintiffs to institute civil proceedings.

3 RELEVANT PROVISIONS OF THE CYBERCRIMES ACT IMPACTING CIVIL PROCEEDINGS

It is submitted that the objectives of the Cybercrimes Act are, *inter alia*, to create and impose penalties on cybercrime, to criminalise the distribution of data messages that are harmful, to provide for interim protection orders, and to regulate jurisdiction further in respect of cybercrime. The provisions of the Cybercrimes Act also regulate powers to investigate cybercrimes (and aspects relating to mutual assistance in respect of the investigation of cybercrimes) and establish a 24/7 point of contact. An obligation is also placed on electronic communications service providers and financial institutions to assist in the investigation of cybercrime.

South Africa's National Executive may also enter into agreements with foreign states to promote measures to address the detection, prevention, mitigation and investigation of cybercrimes. (However, as alluded to in the introduction, this article only addresses those sections or provisions of the Cybercrime Act that the authors view as affecting civil proceedings.) When a defendant unlawfully obtains a plaintiff's confidential data or personal information and commits cyber fraud by using such data, the *facta probanda* and *facta probantia* (that confirm a plaintiff's data was used to commit cybercrimes such as cyber fraud) must be pleaded to illustrate the cause of action. This is notwithstanding that the Cybercrimes Act is mum about civil proceedings.

It is for this reason that the authors wish to convince the legislature to

---

25 *Ibid.*

26 Cassim "Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players" 2011 *Comparative and International Law Journal of Southern Africa* 24.

27 Brenner "Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law" 2001 *Murdoch University Electronic Journal of Law* 1–16.

28 Van der Merwe, Roos, Pistorius, Eiselen and Nel *Communications Technology Law* (2021) 491.

29 Van der Merwe *et al Communications Technology Law* 503.

incorporate a provision that specifically addresses civil proceedings.

Section 9 of the Cybercrimes Act is also significant for potential civil proceedings. When a perpetrator forges a plaintiff's signature to commit a cyberspace crime, such a crime affects the dignity or the good reputation of the plaintiff and such plaintiffs suffer damages as a result. For example, when cybercriminals forge the signature of a plaintiff and implicate such a plaintiff in cybercrime, the good standing and reputation of the plaintiff may be tainted by such implication, particularly if the plaintiff is a professional with a good reputation and is running his own business. Such a plaintiff may lose clients as a result of being implicated in forgery.

It appears that the *facta probanda* and *facta probantia* must be pleaded to prove the cause of action.[30] This means that all relevant or "material facts" that prove or tend to prove that the plaintiff is implicated in the forgery must be incorporated in the pleadings because they amount to a cause of action.[31] Swales argues that "electronic evidence" that affirms *facta probanda* and *facta probantia* ought to be incorporated into the court papers.[32] He further asserts that cybercriminals may manipulate a plaintiff's data or use the plaintiff's electronic signature to commit cybercrime, and he affirms that electronic evidence is real evidence.[33] In an instance of cyber forgery, forged data is regarded as real evidence. Section 9 of the Cybercrimes Act is significant because the Uniform Rules of Court compel parties to plead the cause of action.[34] Thus, *facta probanda* and *facta probantia* must be pleaded in terms of the Uniform Rules of Court.[35]

If this is not done, rule 23 may be invoked. Rule 23 provides for "exceptions and applications to strike out".[36] Just as is the case in the High Court, the rules in the magistrates' courts also compel parties to proceedings to plead and articulate the cause of action. Rule 17 of the Magistrates' Courts Rules is similar to rule 22 of the Uniform Rules of Court. They both force parties to articulate and incorporate *facta probanda* and *facta probantia*. If this does not happen, rule 19 of the Magistrates' Courts Rules may be employed. Thus, parties can file an exception or application to strike out. This may be prejudicial to the plaintiff because they may not be able to recover their damages if the exception or application to strike out is successful. This was illustrated in the case of *Law Society of the Cape of Good Hope v Randell*.[37]

The employment of rule 23 of the Uniform Rules of Court or rule 19 of the

---

30 Broodryk *Eckard's Principle of Civil Procedure in the Magistrates' Courts* 6ed (2019) 26.

31 *Ibid*.

32 Swales "Electronic Evidence" in Papadopoulos and Snail ka Mtuze *Cyberlaw @SA the Law of the Internet in South Africa* 4ed (2022) 435.

33 *Ibid*.

34 Rule 22 of the Uniform Rules of Court, 2009; Rule 17 of the Magistrates' Courts Rules, 1 October 2022.

35 Rule 22 of the Uniform Rules of Court, 2009.

36 Rule 23 of the Uniform Rules of Court, 2009 deals with exceptions and applications to strike out. Rule 19 of the Magistrates' Courts Rules is similar to rule 23 of the Uniform Rules of Court, 2009.

37 (2013) 3 SA 437 (SCA).

Magistrates' Courts Rules in section 9 of the Cybercrimes Act implies that the plaintiff who is a victim of a contravention of the said section may not be able to recover their damages. This is why it is important for the plaintiff to ensure that the cause of action is articulated in the pleadings. This may mean that the same facts used in criminal proceedings may be used in civil proceedings. The case of *Du Toit v Van Rensburg*,[38] as old as it is, is a classic example of courts allowing parties to institute civil proceedings while criminal proceedings are pending.

However, defences are available to a defendant in civil proceedings that may hinder the success of a plaintiff's case when they are raised. For instance, the defendant may raise *lis pendens*[39] or *res judicata*[40] as a special plea.[41] The Supreme Court of Appeal strictly applied the principle of *lis pendens* in *Caesarstone Sdot-Yam v World of Marble and Granite 2000 CC*.[42]

The court held that when all the requirements of *lis pendens* are met, the court will readily dismiss the second proceedings.[43]

Broodryk asserts that

> "the defendant may raise the special defence that an action is already pending between the same parties (or their successors in title) which arises from the same cause of action or in relation to the same subject-matter in dispute."[44]

Pete *et al* concur with Broodryk:

> "[Y]ou cannot sue me for this. You are already suing me for the same reason regarding the same thing. The pending action may be in the same or in different court."[45]

Theophilopoulos *et al* aver that "the court may at its discretion stay the second action subject to the completion of the first".[46]

In addition, the courts may also grant an order for the stay of civil proceedings because the matter is pending, as was the case in *VJ Logistics Services v Fuchs Lubricant*.[47] The defendant, in that case, argued that if the material facts used in the criminal proceedings were also invoked in civil proceedings, he could incriminate himself. The court confirmed the decision in *Du Toit v Van Rensburg*.[48]

---

38 (1967) 4 SA 433 (C) 436.
39 Theophilopoulos *et al Fundamental Principles of Civil Procedure* 205.
40 Theophilopoulos *et al Fundamental Principles of Civil Procedure* 123.
41 Broodryk *Eckard's Principles of Civil Procedure in the Magistrates' Courts* 161.
42 2013 (6) SA 499 (SCA).
43 *Caesarstone Sdot-Yam v World of Marble and Granite 2000 CC supra* par 19–29.
44 Broodryk *Eckard's Principles of Civil Procedure in the Magistrates' Courts* 174.
45 Pete, Hulme, Du Plessis, Palmer, Sibanda and Palmer *Civil Procedure: A Practical Guide* 3ed (2017) 212.
46 Theophilopoulos *et al Fundamental Principles of Civil Procedure* 246.
47 [2020] ZAGPJHC 396 par 3.
48 *Supra*.

Unlike the courts have done, the Cybercrimes Act does not spell out that parties may sue simultaneously in the civil courts while the defendant is facing criminal proceedings. The authors view this as a gap in the Cybercrimes Act because the defences raised as special pleas in civil proceedings may prejudice a plaintiff. For this reason, the authors suggest that there be a specific provision in the Cybercrimes Act that confirms the decision in *Du Toit* to allow a plaintiff to recover damages suffered as a result of a contravention of section 9 without having to worry about the defences that a defendant may raise as a special plea.

Rule 22 provides that the defendant must deny, admit, or confess and avoid the facts comprising the cause of action. When a defendant admits a contravention of section 9 that resulted in a plaintiff suffering damages, such a plaintiff will be entitled to an award of compensation after bringing a civil claim. It is important to interpret the provisions of section 9 in the context of civil procedure. Section 9 provides:

> "(1) Any person who unlawfully and with the intention to defraud, makes–
> *(a* false data; or
> *(b)* a false computer program,
> to *the actual or potential prejudice of another person,* is guilty of the offence of cyber forgery.
> (2) Any person who unlawfully and with the intention to defraud, passes off–
> *(a)* false data; or
> *(b)* a false computer program,
> to *the actual or potential prejudice of another person*, is guilty of the offence of cyber uttering." (own emphasis)

The construction of this provision demonstrates that the consequence of cyber forgery is *prejudice suffered* by the plaintiff, which may result in the loss of large amounts of money; this constitutes a cause of action, and such plaintiff may institute civil proceedings against the defendant. A classic example of the relevance of civil proceedings to this particular provision is the case of *Fourie v Van der Spuy*,[49] where there was unlawful interception conducted by hackers into an attorney's trust account.[50] The thieves gave an instruction to the victims, who were attorneys, pretending to be their clients. The client was unhappy about this, and he sued the attorneys.[51] The court had to decide whether or not the client was implicated in the cybercrime because he refused to provide his laptop to the attorneys.[52] The court concluded that the attorneys failed to honour their duty to check the authenticity of the instructions.[53] Damages were accordingly awarded to the client.

In another case, *Global & Local Investments Advisors (Pty) Ltd v Fouche,*[54] Fouche had concluded "a written mandate" with Global that any

---

49 *Fourie v Van der Spuy* (2020) 1 SA 560 (GP).
50 *Fourie v Van der Spuy supra* par 1–5.
51 *Ibid*.
52 *Fourie v Van der Spuy supra* par 8.
53 *Fourie v Van der Spuy supra* par 30 and 31.
54 2021 (1) SA 371 (SCA).

withdrawal instruction would be in writing and signed by Fouche.[55] Hackers sent emails with instructions to withdraw, but these emails did not have Fouche's signature and ended with the word "Nick".[56] The Supreme Court of Appeal held that the withdrawal instruction given by hackers was indeed "fraudulent". According to the court, Fouche was entitled to repayment of the money that had been withdrawn by cyber thieves. It is observed that section 9 is silent as to whether a plaintiff may concurrently institute civil action after opening a criminal case against the defendant. It is the authors' view that there should be an amendment to the Cybercrimes Act to allow parties to use both criminal and civil proceedings concurrently.

Section 19 of the Cybercrimes Act provides for penalties when it is proved that there is a contravention of the said provisions.[57] The relevant provision for present purposes is section 19(4). This subsection gives the courts the discretion to impose penalties for a contravention of section 9 (among others) where a penalty is not prescribed in respect of that offence by any other law.[58] This provision does not refer to damages or compensation that may be awarded to the plaintiff when section 9 is contravened and where there is a civil claim based on the same cause of action. The authors submit that this provision should be amended to allow courts to award damages suffered as a result of a contravention of section 9 of the Cybercrimes Act and that plaintiffs should not need to worry about the defences that may be raised as a special plea in civil proceedings. The authors have identified this as a gap that must be corrected in the Cybercrimes Act.

Section 16 is crucial in interpreting the provisions of the Cybercrimes Act in the context of civil proceedings: the consequences of a breach of section 16 may have dire consequences for the plaintiff. He or she may suffer damages that destroy his or her standing and good reputation, as was the case in *Le Roux v Dey*.[59] Section 16 states:

> "(1) Any person (**'A'**) who *unlawfully and intentionally discloses*, by means of an electronic communications service, a data message of *an intimate image* of a person (**'B'**), *without the consent* of B, is guilty of an offence.
>
> (2) For purposes of subsection (1)–
>
> *(a)* **'B'** means–
>
> (i) the person who can be identified as being displayed in the data message;
>
> (ii) any person who is described as being displayed in the data message, irrespective of the fact that the person cannot be identified as being displayed in the data message; or
>
> (iii) any person who can be identified from other information as being displayed in the data message; and
>
> *(b)* **'intimate image'** means a depiction of a person–
>
> (i) real or simulated, and made by any means in which–
>
> *(aa)* B is nude, or the genital organs or anal region of B is displayed, or if B is a female person, transgender person

[55] *Global & Local Investments Advisors (Pty) Ltd v Fouche supra* par 2.
[56] *Global & Local Investments Advisors (Pty) Ltd v Fouche supra* par 3.
[57] S 19 of the Cybercrimes Act.
[58] S 19(4) of the Cybercrimes Act.
[59] (2011) 3 SA 274 (CC).

or intersex person, their breasts, are displayed; or

(bb) the covered genital or anal region of B, or if B is a female person, transgender person or intersex person, their covered breasts, are displayed; and

(ii) in respect of which B so displayed retains a reasonable expectation of privacy at the time that the data message was made in a manner that–

(aa) violates or offends the sexual integrity or dignity of B; or

(bb) amounts to sexual exploitation." (own emphasis)

Section 16 of the Cybercrimes Act is just as significant as section 9 because the consequences of a contravention of this section may result in a plaintiff incurring damages that give rise to a cause of action that may allow parties to institute civil proceedings against the defendant who publishes intimate images on social media and cyberspace without obtaining permission from the plaintiff.[60]

The case of *Le Roux v Dey* is a classic example of the application of section 16; here, schoolchildren distributed manipulated pictures of bodybuilders into which they inserted Dr Dey's picture, insinuating that he was involved in a gay relationship.[61] Dr Dey was very unhappy about this, and he sued the defendants. The court agreed that the pictures damaged his dignity.[62]

The Supreme Court of Appeal confirmed that the distribution of the photographs amounted to a cause of action that entitled Dr Dey to compensation.[63]

In the recent case of *Ramokgopa v Nxumalo*,[64] although not dealing with section 16 of the Cybercrimes Act *per se*, the court considered WhatsApp messages that were distributed at the University of Cape Town and in which the plaintiff was labelled as a rapist and an assaulter. The WhatsApp group to which the plaintiff belonged informed him that he would no longer belong to the group because he was a rapist.[65] The court confirmed that WhatsApp is an electronic instrument used to communicate with others.[66] This case illustrates that section 16 applies where it is proved that a breach of this kind results in substantial damages. Thus, the person who distributes derogatory statements or intimate images on WhatsApp is, in reality, breaching section 16 of the Cybercrimes Act.

In *Manyi v Dhlamin*i,[67] harmful comments such as "horny stinky donkey" that humiliated and degraded the dignity of the plaintiff were distributed on Whatsapp.[68] The High Court awarded damages to the plaintiff in the amount

---

60 *Isparta v Richter* 2013 (6) SA 529 (GNP) par 12, 13 and 14.

61 *Le Roux v Dey supra* par 13–14.

62 *Ibid*.

63 *Le Roux v Dey supra* par 78.

64 [2022] ZAWCHC 175.

65 *Ramokgopa v Nxumalo supra* par 6, 13, 14, 31–34.

66 *Ramokgopa v Nxumalo supra* par 31–34.

67 *Supra*.

68 *Manyi v Dhlamini supra* par 5.

of R50 000 because it was satisfied that the plaintiff had indeed suffered damages. This case shows that there should be a provision under section 16 of the Cybercrimes Act for a simultaneous civil claim for damages when there is a violation in this regard. The point is made because, for various reasons, criminal proceedings or trials may take a long time to be finalised.

The plaintiff should be allowed to institute proceedings while the matter is pending in the criminal courts, and the defendant should not be permitted to raise a special plea as a defence on the grounds that the matter is still pending before the criminal courts. This should be incorporated into the provisions of the Cybercrimes Act.

Authors such as Iyer,[69] Milo,[70] Nel[71] and Skibell[72] argue that publishing derogatory statements on social media such as Facebook, Twitter, and other means of social media enables the plaintiff to argue successfully in civil proceedings for damages.[73] Iyer asserts that the plaintiff may use the *actio iniuriarum* to claim damages that arise from cyber defamation.[74] In addition, insults posted on Facebook are viewed as derogatory and affect the "personality rights" and good reputation of a plaintiff.[75] Iyer refers to the Cybercrimes Act and argues that publishing harmful data is viewed as a criminal offence.[76]

It is important to interpret the provisions of section 17 of the Cybercrimes Act in the context of civil procedure. Section 17 states:

> "Any person who *unlawfully and intentionally*–
> *(a)* attempts;
> *(b)* *conspires* with any other person; or
> *(c)* aids, abets, induces, incites, *instigates*, instructs, commands or procures another person, to commit an offence in terms of Part I or Part II of this Chapter, is guilty of an offence and is liable on conviction to the punishment to which a person convicted of actually committing that offence would be liable." (own emphasis)

The construction of this provision shows that the intention of the legislature is to enable a civil action based on a civil claim that stems from the consequences of a contravention of section 17.

It is, however, noted that this stipulation does not expressly indicate

---

69 Iyer "An Analytic Look into the Concept of Online Defamation in South Africa" 2018 *Speculum Juris* 125–134.

70 Milo "It's Hard for Me to Say I'm Sorry: Apology as a Remedy in the South African Law of Defamation" 2015 *Journal of Media Law* 11–16; Milo "Case Law, South Africa: *Manuel v Economic Freedom Fighters and Others*" (6 June 2019) https://inforrm.org/2019/06/06/case-law-south-africa-manuel-v-economic-freedom-fighters-the-legal-consequences-of-fake-news-dario-milo/ (accessed 2021-06-06) 1.

71 Nel "Defamation on the Internet and Other Computer Networks" 1997 *CILSA* 154–174; Nel "Rath v Rees 2006 CLR 429 (C)" 2009 *De Jure* 341–352.

72 Skibell "Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act" 2003 *Berkeley Technology Journal* 909–944.

73 Iyer 2018 *Speculum Juris* 125–134; Milo 2015 *Journal of Media Law* 11–16; Nel 1997 *CILSA* 154–174; Nel 2009 *De Jure* 341–352.

74 Iyer 2018 *Speculum Juris* 127–134.

75 *Ibid*.

76 *Ibid*.

that civil proceedings should be capable of running concurrently with criminal matters. It is the view of the authors that the Cybercrimes Act should clearly state that a plaintiff may institute civil proceedings when they suffer damages as a result of a contravention of this provision.

In the case of *Heroldt v Willis,*[77] a wife published derogatory statements on Facebook. The wife labelled the husband a bad father and indicated that he was not supporting his children.[78] The court agreed with the husband that the statements made on Facebook were indeed derogatory and damaged his reputation.[79] An interdict was granted to force the wife to remove the statements on Facebook.[80]

In the case of *Manuel v Economic Freedom Fighters*, derogatory statements were published on Twitter.[81] Although this case did not specifically deal with the construction or contravention of section 17, it shows that those who instigate and conspire against plaintiffs in cyberspace, such as social media, may be held accountable. The court noted that the plaintiff in this case averred:

> "The statement is highly defamatory of him, as well as Mr Kieswetter and other members of the panel, as the statement implies that he:
> (a) is corrupt,
> (b) is nepotistic,
> (c) conducted 'secret interviews' and participated in a secretive process to select the new SARS Commissioner;
> (d) conducted an unlawful appointment process, which led to the appointment of Mr Kieswetter as the SARS Commissioner, who was not deserving of the appointment;
> (e) made previous unlawful appointments to positions at SARS during his tenure as Minister of Finance;
> (f) is connected to a 'white capitalist establishment' that acts contrary to the best interests of SARS."[82]

The court agreed that the respondent ought to apologise to the applicant. In addition, the court awarded compensation in favour of the applicant. It is submitted that the decision of the court is correct, and it falls within the ambit of the construction of the provisions of section 17 of the Cybercrimes Act. It is submitted that the plaintiff should also not be prevented from simultaneously instituting a claim for damages in civil proceedings. The authors suggest that there is a need to amend this provision to incorporate a reference to simultaneous civil proceedings.

It is noteworthy that Part VI of the Cybercrimes Act (which provides for orders to protect a claimant who is the subject of malicious communications) only addresses criminal sanctions. Although the Cybercrimes Act was

---

77 (2014) JOL 31479 (GSJ) par 43–47.

78 *Ibid*.

79 *Heroldt v Willis supra par* 45–47.

80 *Ibid*.

81 *Manuel v Economic Freedom Fighters* (2019) 3 All SA 584 (GJ) par 1–18; Milo https://www.inforrm.org/2019/06/06/case-law-south-africa-manuel-v-economic-freedom-fighters-the-legal-consequences-of-fake-news-dario-milo/.

82 *Manuel v Economic Freedom Fighters supra* par 35.

designed to deal with criminal proceedings, it is however apparent that the consequences of contraventions may result in substantial damages to a plaintiff. A plaintiff should thus be allowed to institute civil proceedings simultaneously. It is the authors' view that this should be incorporated into the provisions of the Cybercrimes Act, so a plaintiff is able to institute both criminal and civil proceedings in terms of the Cybercrimes Act without having to worry about the civil procedure defences.

4 A BRIEF COMPARATIVE ANALYSIS OF THE CYBERCRIMES ACT AND THE BUDAPEST CONVENTION

The Council of Europe's Convention on Cybercrime was opened for signature on 23 November 2001 in Budapest, hence known as the Budapest Convention. It strives to encourage countries to combat cybercrime. It has been described as the first international treaty on crimes that are committed via the Internet and other computer networks.[83]

It strives to advance a common criminal policy aimed at the protection of society from cybercrime by adopting appropriate legislation and fostering international cooperation.[84]

Article 8 addresses computer-related fraud and incorporates the use of legislative and other measures to address criminal offences resulting in loss of property to another person. Article 13 addresses sanctions and measures and incorporates the employment of effective and proportionate criminal or non-criminal sanctions, including monetary sanctions.[85] It is submitted that the use of the phrase "non-criminal sanctions" is wide enough to include civil sanctions or remedies in article 13. Moreover, article 13's provisions are akin to section 23[86] of the Cybercrimes Act because they both seek to prohibit cybercrimes by imposing sanctions, fines and even imprisonment where necessary. However, article 13 refers to "non-criminal" sanctions or measures, meaning that civil proceedings may be invoked where there is evidence that the cause of action arose from a cybercrime.

Unlike article 13, section 23 does not specifically refer to "non-criminal" sanctions. It is submitted that section 23 should follow a similar approach and expressly incorporate a provision that refers to civil proceedings. This would entrench the decision taken by the courts in the *Du Toit* and *Heroldt* cases,[87] empowering plaintiffs to sue without worrying about civil procedure defences that may be raised as a special plea. This is because defendants may raise a special plea available in civil proceedings (such as *res judicata*)

---

83 Cassim "Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players" 2014 *CILSA* 423.

84 Cassim 2011 *CILSA* 126.

85 Art 13.2 of the Budapest Convention.

86 S 23 states: "[A]ny person or electronic communications service provider that is convicted of an offence referred in section 20(9) or (10), 21(7) or 22(4) or (8), is liable on conviction to a fine or to imprisonment for a period not exceeding two years or to both a fine and such imprisonment."

87 *Supra.*

when a plaintiff institutes a civil claim stemming from a cause of action that arises from a contravention of the provisions of the Act. The defence raised may hinder the plaintiff from recovering damages suffered.

Article 35 of the Convention addresses the use of a 24/7 point of contact to promote effective cooperation.[88] National 24/7 points of contact that are adequately capacitated and manned with properly trained and equipped personnel can be used to transmit requests and responses for assistance from member states and reduce challenges associated with delays associated with requests for assistance by member states.

If the States Parties are able to use expedited means of communication as envisaged under article 25 (such as a fax, email or even phone call) and the requested state also communicates its response through the same expedited means of communication, then the problem of delay with requests for assistance by member states should also be minimised. Similarly, South Africa needs to ensure that the 24/7 points of contact are adequately manned and resourced.

Ambrose *et al*[89] assert that the Budapest Convention is significant for civil proceedings because evidence is an aspect of litigation in civil proceedings.[90] The Convention provides a way to ensure that evidence is obtained in matters concerning cybercrimes.[91] Thus, *facta probanda* and *facta probantia* must be pleaded in terms of the rules.[92] This means that the same cause of action used in criminal proceedings may also be used in civil proceedings. The pleaded facts thus form part of civil litigation, and in terms of rule 21 of the Uniform Rules of Court, these may be requested to substantiate a civil claim whose cause of action arises from cybercrimes.[93]

It is therefore evident that the doctrine of effectiveness is promoted by ratification of the Budapest Convention. South Africa has adopted the Budapest Convention but has not ratified it. South Africa has, to a certain extent, complied with the Budapest Convention because the stipulations of the Cybercrimes Act are drafted to prevent unlawful computer crimes. It is submitted that South Africa should consider incorporating in section 23 of the Act a specific provision that allows for "non-criminal sanctions". This will bring the Cybercrimes Act in line with the Budapest Convention.

5 CONCLUSION

The Cybercrimes Act was enacted to create "new crimes" in the form of the cybercrimes highlighted in the article and to place a positive obligation on the State to deal with these crimes. The President assented to the Cybercrimes Act on 1 June 2021 and it is now in operation.

---

88 This is similar to Ch 6 of the Cybercrimes Act.

89 Ambrose, Browne, Kean, Laurenti, Lidbetter, McMeel, Naish, Owens, Pertoldi, Scott and Taylor *Blackstone's Civil Practice* (2021) 1106.

90 *Ibid*.

91 *Ibid*.

92 *Ibid*.

93 Rule 21 deals with the request for further particulars.

It has been observed that there is a common gap in the provisions of sections 9, 19 and 16 of the Cybercrimes Act insofar as the institution of civil proceedings is concerned. This is why the authors express the view that the provisions of the Cybercrimes Act should include the possibility of instituting simultaneous action in civil proceedings without a plaintiff needing to worry about defences raised as a special plea that may stop them from recovering substantial amounts of money lost as a result of the contravention of the above-mentioned stipulations.

The gap that has been identified is that the Act does not articulate whether civil proceedings may be instituted simultaneously with criminal proceedings. It is submitted that the plaintiff should be allowed to institute civil proceedings while criminal proceedings are pending. Perpetrators should not be allowed to raise civil procedure defences to raise a successful special plea.

The case law (such as *Heroldt v Willis, Le Roux v Dey*, and *Manuel v Economic Freedom Fighters*)[94] illustrates that the South African courts follow a strict approach to cyberspace matters. The authors also argue that cyber criminals cause misery to their victims because the damage caused by cyber fraud, theft, forgery and distribution of personal data without consent costs the victim a lot of money and causes damage to their reputation.

Trial proceedings may take up to three years before being finalised in practice, and by that time, attorneys' costs paid by a plaintiff may have reached very large amounts. Thus, plaintiffs are prejudiced by long and expensive trial proceedings. Therefore, the gap should be addressed by the legislature. Although courts allow civil proceedings to run simultaneously, as in the *Du Toit* case, the Cybercrimes Act does not refer to this. This leaves room for the employment of defences that may prejudice a plaintiff. These may prevent a plaintiff from claiming the damages resulting from a breach of the Cybercrimes Act. The future journey suggested in this article is the modification of the Cybercrimes Act expressly to allow for civil proceedings claims when these are based on the same cause of action or the same material facts that must be pleaded in terms of the rules of the superior and lower courts for criminal proceedings.

Lastly, it is concerning that the Cybercrimes Act does not address non-criminal sanctions as the Convention on Cybercrime does. It is submitted that the Cybercrimes Act should also introduce non-criminal sanctions into its provisions and that South Africa should ensure that the 24/7 points of contact are adequately resourced and effective.

94 *Supra.*