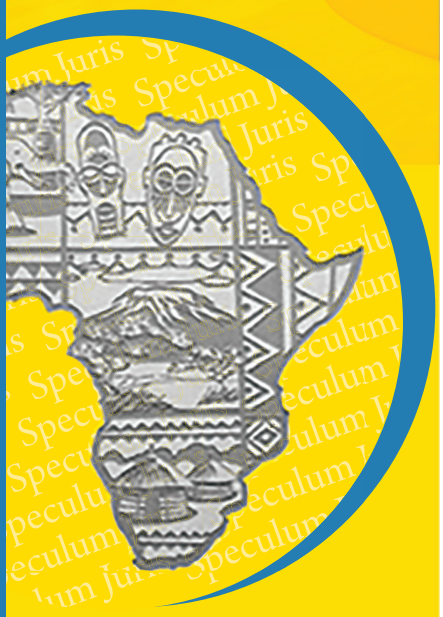
Speculum Juris



University of Fort Hare
Together in Excellence

Editorial Board

Prof Mzukisi Njotini, Chairperson of the Board,

Professor and Dean of Law, University of Fort Hare

Prof Patrick C. Osode, Managing Editor,

Professor of Law, University of Fort Hare

Prof Nomthandazo Ntlama-Makhanya, Member,

Professor of Law, University of Fort Hare

Prof Enyinna S. Nwauche, Member,

Professor of Law, University of Fort Hare

Prof Arthur van Coller, Associate Editor,

Associate Professor of Law, University of Fort Hare

Dr Simphiwe S. Bidie, Associate Editor,

Senior Lecturer in Law, University of Fort Hare

Dr Tapiwa Shumba, Associate Editor,

Senior Lecturer in Law, University of Fort Hare

Dr Nombulelo Lubisi-Bizani, Associate Editor,

Senior Lecturer in Law, University of Fort Hare

Dr Ntandokayise Ndhlovu, Associate Editor,

Senior Lecturer in Law, University of Fort Hare

Adv Shandukani Muthugulu-Ugoda, Associate Editor,

Senior Lecturer in Law, University of Fort Hare

Adv Sibulelo Seti, Associate Editor,

Senior Lecturer in Law, University of Fort Hare

Ms Lulama Gomomo, Assistant Editor,

Lecturer in Law, University of Fort Hare

Ms Asanda Mbolambi, Assistant Editor,

Lecturer in Law, University of Fort Hare

Speculum Juris

ISSN 2523-2177 • Volume 38, Number 2 (2024)

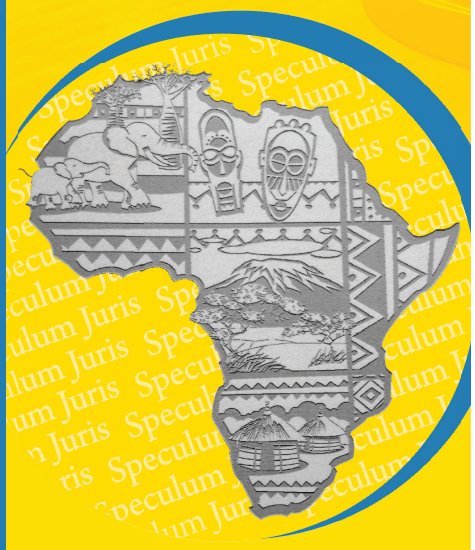
Articles

Notes and Comments

Speculum Juris

Vol 38 No 2 (2024)
Published 31 December 2024

ISSN 2523-2177



University of Fort Hare
Together in Excellence

Cite as: Mabeka "The Cybercrimes Act 19 of 2020, Section 7 versus Civil Proceedings" 2024 (38) Spec Juris 419–436

The Cybercrimes Act 19 of 2020, Section 7 versus Civil Proceedings

Nombulelo Queen Mabeka*
Associate Professor, Department of Jurisprudence, University of South Africa

Abstract

The provisions of section 7 of the Cybercrimes Act 19 of 2020 (hereinafter referred to as the Act) shield the unlawful acquisition or possession of passwords. The different forms of attacks such as "dictionary-based attacks" threaten the protection of passwords because hackers can obtain confidential data through these attacks without using a password. Methods like "phishing" add another risk to section 7 of the Act because hackers do not need to have a password to obtain confidential data such as a client's banking details . Digital snooping is another serious concern in the application of section 7 of the Act in the context of civil proceedings. The consequences of a contravention of section 7 of the Act constitute a cause of action that enables the plaintiff to claim damages. If the defendant is already convicted or sentenced for such a contravention, he/ she may raise a special plea based on res judicata. This defence blocks the plaintiff from recovering the damages suffered because of a contravention of section 7 of the Act. A gap is thus identified, in that there is no provision in the Act that allows the plaintiff who has suffered substantial damages to institute civil proceedings over and above the criminal proceedings that are instituted against the defendant. This article interprets the stipulations of section 7 of the Act in the context of civil procedure to determine availability of the cause of action. I examine the legal position in the United Kingdom and

* LLB, LLM (UWC) LLD (UNISA), Admitted Attorney of the High Court.

compares this jurisdiction with South Africa. Lastly, the author sets out factors that should be considered by the courts to ensure that justice prevails.

Keywords: Cybercrimes Act, section 7; civil procedure; *res judicata*: special plea; cause of action; United Kingdom; RIPA and Factors

1 INTRODUCTION

The Cybercrimes Act 19 of 2020[1] has just come at the right time because cyber criminals are attacking various jurisdictions and the victims suffer dire financial consequences.[2] The conviction and sentencing provided in the Act do not always satisfy the plaintiffs or the victims.[3] Some lose exorbitant amounts of money, which they cannot recover.[4] The best way of recovering money lost because of a contravention of section 7 of the Act is to institute civil proceedings against the perpetrators or defendants.

The consequences of a contravention of the stipulations of section 7 constitute a cause of action when interpreted in the context of civil procedure and this enables the plaintiff to sue.[5] For example, if defendants are already convicted and sentenced in terms of the Act and the plaintiff subsequently institutes civil litigation against such defendants, the latter may raise *res judicata* as a special plea. It must be pointed out that section 7 must be read with section 4(1) of the Cybercrimes Act because there is specific reference to section 7(1)(a) and (d) in the said section. Section 4 provides that it is an offence to act against the law in relation to "software or hardware tool".

The question that is asked is, should the courts do away with *res judicata* when there is substantial evidence that confirms that the plaintiff has suffered severely as a result of the contravention of section 7? This article attempts to answer this question by first interpreting the provisions of section 7 of the Act in the context of civil procedure. Thereafter, I compare South African law with that of the United Kingdom. This article further sets out factors that should be considered by the courts and concludes by highlighting important aspects.

2 ANALYSIS OF THE PROVISIONS OF SECTION 7 OF THE ACT

Before embarking on the interpretation of the provisions of section 7 of the Act, it is important to briefly highlight the significance of passing this Act. Section 19 of the Cybercrimes Act aims

1 Hereinafter referred to as The Act.

2 Cassim "Addressing the Growing Spectre of Cybercrimes in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players" 2011 *CILSA* 123138.

3 Section 23 of the Cybercrimes Act, which provides for penalties; Papadopoulos, Snail and Mtuze *Cyberlaw@SA Cyberlaw@SA the Law of the Internet in South Africa* (2021) 480.

4 Cassim 2011 *CILSA* 130.

5 *Ibid* 127.

to regulate cybercrimes and it provides sentences that should be imposed on the perpetrators.[6]

Section 7 deals with cybercrimes that are committed by illegally obtaining a person's password.[7] Section 7 states that:

> (1) Any person who *unlawfully* and *intentionally*-
>
> *(a)* acquires;
>
> *(b)* possesses;
>
> *(c)* provides to another person; or
>
> *(d)* uses, a password, an access code or similar data or device for purposes of *contravening the provisions* of section 2(1) or (2), 3(1), 5(1), 6(1), 8 or 9(1), is guilty of an offence.
>
> (2) Any person who is found *in possession of a password, an access code or similar*
>
> *data or device* in regard to which there is a reasonable suspicion that such password, access code or similar data or device—
>
> *(a)* was acquired;
>
> *(b)* is possessed;
>
> *(c)* is to be provided to another person; or
>
> *(d)* was used or may be used, for purposes of contravening the provisions of section 2(1) or (2), 3(1), 5(1), 6(1), 8 or 9(1), and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence…

Before interpreting the above section, it must be elucidated that section 7 must be read with section 4(1) of the Cybercrimes Act. Section 4(1) makes it an offence to keep or use software to commit cybercrime in a manner that is set out in section 7. It is imperative to note that section 7 should be contextually construed. For example, the use of words such as "unlawful" and "intentionally" shows that it was the intention of the legislature to prevent and prohibit unlawful acquiring of passwords. The same applies to those in possession of passwords, which are obtained in a manner that is against the law — the illegal possession itself is a contravention of the stipulations of section 7 of the Act.

Further, those who give passwords to others for committing cybercrime are breaking the law in terms of section 7 of the Act. In addition, when a person uses a password that does not belong to them to commit cybercrime such a person contravenes section 7.

It is borne in mind that section 300 of the Criminal Procedure Act 51 of 1977 (CPA) provides that prosecutors may apply and ask the court to compensate the victim. The question is, what happens when the amount awarded by the court in criminal proceedings is not enough to cover the damages suffered by the plaintiff? Can such a plaintiff institute civil proceedings against the same defendant for the damages that are not covered in terms of section 300. These questions are raised because of the limited jurisdiction of the lower courts. It is submitted that if the compensation awarded by the criminal courts does not cover all the damages suffered by the plaintiff as a consequence of the contravention of section 7 of the Act, such plaintiff may

6 Section 19(1) of the Cybercrimes Act; Watney "Cybercrime" 480 in Papadopoulos *et al*. *Cyberlaw@SA* 480; Snail 'kaMtuze and Musomi "An Overview of Cybercrime Law in South Africa" 2023 *International Cybersecurity LR* 299–323.

7 Section 7 of the Act.

institute civil proceedings to claim the remainder of the damages that are not covered in the compensation awarded in terms of section 300 of the CPA.

The court in *Du Toit v Van Rensburg* stated that if there is prejudice suffered by the accused who is a defendant in civil proceedings, the court will stay the civil proceedings.[8] In the recent case of *VJ Logistics Services v Fuchs Lubricants South Africa (Pty) Ltd*,[9] the court held that criminal and civil procedure may be conducted simultaneously. The court was satisfied that "… it is proper that both the civil proceedings and criminal proceedings run concurrently…".[10] The analogy of these cases demonstrates that the courts will allow a civil claim instituted to recover the rest of the damages after section 300 of the CPA is applied in criminal proceedings.

The court in *Geber v PSGP Wealth Financial Planning (Pty) Ltd*[11] averred that for security reasons, passwords should not be used unchanged for a long period because hackers might intercept the system. In the case of *Hawarden v Edward Nathan Sonneburg Inc*,[12] the court confirmed that it is crucial to take due care when using passwords to prevent the risk of hacking. Van der Merwe et al. agrees that a contravention of section 7 is an offence that is punishable in terms of the Act.[13]

Mabunda states that "the possession of any passwords, access codes and the like where there is a reasonable suspicion that such were acquired, possessed, provided or used to commit the offenses" constitutes an offence in terms of section 7 of the Cybercrimes Act.[14] Mabunda says section 7(3) is described as an "acknowledgement, the development of technology and possibilities that exist in the future of cybercrime".[15] Nnaemeka asserts that phishing is the latest tool used by cybercriminals and "… it's a method that hackers employ to steal private data, including credit card information, usernames, passwords, PINs, bank account numbers, and other details. Phishing is frequently carried out using email spoofing, which is the use of false emails that ask the user to provide certain information …".[16]

Snail ka Mtuze argues that section 7 of the Cybercrimes Act is linked to data protection in terms of the Protection of Personal Information Act 4 of 2013.[17] Snail indicates that data protection must be enforced. Sekhar and Kumar assert that spoofing is another method used to steal data stored by the banks.[18] Notwithstanding the fact that section 7 protects data by password encryption, there is still a big risk that confidential data may be stolen without using a password.

The risk imposed by the compromise of the password may lead to unlawful interception. Section 2 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) prevents the interception conducted without permission and in a manner that is against the law. Section 49 of RICA endorses the provisions

8 1967 4 SA 433.

9 *VJ Logistics Services v Fuchs Lubricants South Africa (Pty) Ltd* [2020] ZAGPJHC 396, para 18 and 22.

10 *VJ Logistics Services* case, para 22.

11 Case no: 36447/2021 (2023) ZAGP JHC 270, para 88.

12 2023 1 All SA 675 GJ, para 127.

13 Van der Merwe *et al. Information and Communications Technology Law* (2021) 91.

14 Mabunda "The South African Legislative Response to Cybercrime" (LLD-thesis, UWC, 2021) 98.

15 *Ibid* 99.

16 Nnaemeka "Cybercrime and Online Safety: Addressing the Challenges and Solutions related to Cybercrime, Online Fraud, and Ensuring a Safe Digital Environment for All Users" 2023 *TIJER* (International Research Journal) 980.

17 Snail Sizwe kaMtuze "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 2013" 2022 *Obiter* 536–569.

18 Sekhar and Kumar "An Overview of Cyber Security in Digital Banking Sector" 2023 East Asian Journal of Multi-disciplinary Research 43–52.

of section 2 of RICA by making unlawful interception an offence. These provisions are akin to the stipulations of sections 2 and 3 of the Act. Section 2 makes it an offence to have unlawful access to a computer. This is usually the case where cyber criminals hack computers and gain access to a system without permission. It appears that section 2 of the Act tacitly endorses the provisions of section 7 of the Act. Section 3 of the Act prevents interception conducted in a manner that is against the law.

The following cases show the damage to the victims caused by hacking. The case of *Jurgens and Another v Volschenk*[19] is a classic example of damages suffered because of hacking. Briefly, in this case, the legal practitioners were ordered to pay an exorbitant amount of money to the client who suffered damages due to hacking.[20] In *Fourie v Van der Spuy and De Jongh Inc. and Another* the legal practitioners' emails were "hacked".[21] The plaintiff in this case suffered damages by way of withdrawals made from the trust account of the legal practitioners that the plaintiff was not aware of.[22] The court decided in favour of the plaintiff.[23]

Another case that shows damages suffered by the victims of hacking is *Global & Local Investments Advisors (Pty) Ltd v Fouche*.[24] The emails between Global & Local Investments and Mr Fouche who signed an investment agreement or mandate were hacked.[25] Instructions for withdrawals were given by hackers and payments were made into their account.[26] The Supreme Court of Appeal endorsed the decision of the high court to pay Mr Fouche for the damages he suffered as a result of hacking.[27]

The case of *Geber v PSG Wealth Financial Planning (Pty) Ltd*[28] is akin to the *Global & Local Investment* case. Emails were hacked by cybercriminals and there were investment withdrawals made that the plaintiff was not aware similar to Mr Fouche's case.[29] Resultantly, the plaintiff suffered damages and the court order that the plaintiff be paid back the amount of damages suffered.[30]

The court asserted that the legal practitioners ought to have double-checked the bank details that the hackers sent and because this was not done, the plaintiff was entitled to receive the amount suffered as damages.

In *Hartog v Daly and Others*,[31] there was "business email compromise".[32] The emails between the appellant and the respondent were intercepted in a manner that was against the law. The money that should have been paid into the correct account was paid into the cybercriminals' account. The court decided in favour of the respondent and validated the payment due to the

19 Case no: 4067/18 2019 ZAECPEHC (27 June 2019).

20 *Jurgens and Another v Volschenk* Case no: 4067/18 2019 ZAECPEHC (27 June 2019) para 26.

21 2020 1 SA 560 (GP).

22 *Fourie v Van der Spuy and De Jongh Inc. and Another* 2020 1 SA 560 (GP) para 1.

23 *Fourie* case para 31.

24 2021 1 SA 371 (SCA).

25 *Global & Local Investments Advisors (Pty) Ltd v Fouche* 2021 1 SA 371 (SCA) para 3.

26 *Ibid.*

27 *Global & Local Investments Advisors* case, para 16.

28 Case no: 36447/2021 2023 ZAGPJHC 270 (23 March 2023).

29 *Geber v PSG Wealth Financial Planning (Pty) Ltd* Case no: 36447/2021 2023 ZAGPJHC 270 (23 March 2023) para 2.

30 *Ibid* para 103.

31 2023 2 All SA 156 (GJ).

32 *Hartog v Daly and Others* 2023 2 All SA 156 (GJ) paras 8 and 75.

latter.[33] In *Edward Nathan Inc v Hawarden*,[34] the Supreme Court of Appeal took a different approach in awarding damages on instances where the plaintiff had been warned of cybercrime. The court refused to endorse the decision of the high court that awarded damages to the plaintiff because the latter had been warned by legal practitioners about cybercrime.[35]

Voiskounsky and Smyslova argue that hackers use different methods.[36] They all aim to obtain software to access data and information of the victim without permission.[37]

These hackers do not need a password to hack the victims.[38] Snail states that cybercriminals use "viruses, worms and Trojan Horses" to hack computers without using a password.[39] Evidently, this is concerning for the interpretation and application of section 7 stipulations.

Consequently, cybercriminals may obtain data and use it to commit cyber fraud, which may result in damages to the plaintiff. Chitimira and Ncube[40] argue that cybercrime such as money laundering in South African banks affects the victims.[41] Pillay *et al*[42] concur with Chitimira and Ncube that banks are targeted more frequently by hackers and cybercriminals.

These authors indicate that hackers do not need a password because they obtain the bank's information through "phishing", "vishing", "spam" and so forth.[43]

The strict application of section 7 denotes that the plaintiff may not necessarily have a recourse when the defendant who hacked and used the plaintiff's data to commit the crime is convicted or sentenced under the said Act. This calls for an amendment of the provisions of section 7 of the Act. There should be a proviso that allows the plaintiff to institute civil proceedings against the defendant who is convicted or sentenced for contravening section 7 of the Act. This will enable the plaintiff to recover damages suffered because of hacking. The same applies to subsection 2, which states that a person who is in possession of a password and suspects that such a password was not legally obtained, is contravening section 7(2) of the Act. When this provision is construed in a civil procedure context, it appears that a contravention of section 7(2) and (3) respectively of the Act constitutes a cause of action, which enables the plaintiff to sue the defendant to recover damages suffered as a result of such contravention.

It appears that the consequences of a contravention of the Act amount to a cause of action. Cassim and Mabeka state that:

> 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

33 *Ibid* para 81.

34 *Edward Nathan Sonnenberg Inc v Hawarden* (421/2023) 2024 ZASCA 90 (10 June).

35 *Ibid* para 25.

36 Voiskounsky and Smyslova "Flow-Baseed Model of Computer Kackers Motivation" 2003 *CyberPsychology & Behaviour* 171–180.

37 *Ibid*.

38 *Ibid*.

39 Snail "Cybercrime in South Africa: Hacking, Cracking, and Other Unlawful Online Activities" 2009 *Journal of Information, Law & Technology* 3.

40 Chitimira and Ncube "The Regulation and use of Artificial Intelligence and 5G Technology to Combat Cybercrime and Financial Crime in South African Banks" 2021 *PELJ* 1–33.

41 *Ibid*.

42 Pillay, Ntuli and Ehiane "Exploring the Prevalence of Cybercrime in Banking Industry in KwaZulu-Natal, South Africa" 2023 *International Journal of Membrane Science and Technology* 1763–1775.

43 *Ibid* 1766.

> mum about civil proceedings.[44]

I concur with the above assertion because the clients may suffer damages because of a contravention of section 7 of the Act. The clients who suffer damages should be permitted to institute civil proceedings.

It is important to state that the methods of password attacks grossly violate the provisions of section 7 of the Act. Brar and Kumar argue that password attacks pose a huge risk to protecting data.[45] They indicate that:

> Password-based attacks are used to get the username and password of authorised users of an application, website, desktop computers, and laptops. These captured usernames and passwords are further used to get access to network services as authorized user and to do malicious act.[46]

Brar and Kumar further assert that there are three different methods of password attacks that may be used to unlawfully acquire data,[47] namely, "dictionary-based attack" and this is described as a method where:

> … an attacker tries every combination of characters or words as defined in the dictionary to hack passwords of authorized users of Internet resources or applications. This type of attack result depends on the authorized user's password. If the user does not choose passwords similar to dictionary words, then it is almost impossible for the attacker to hack the password of the user with this attack …[48]

Furthermore, "brute-force attack" is described as a method by which:

> … an attacker tries every single possible password combination using brute-force hacking tools to hack the user password. This technique is time-consuming but results in the hacking of the authorized user's password. This attack can take few seconds to few days or few months also according to the complexity of passwords …[49]

In addition, "guessing attack" is regarded as a method whereby "an attacker tries to guess the passwords of authorized users by using common words like date of birth, name, and religion".[50]

Kumar indicates that cybercriminals unlawfully acquire data through phishing.[51] The most common method that is employed by hackers is the guessing attack.[52] Brar and Kumar indicate that:

---

44 Cassim and Mabeka "Interpreting the Provisions of the Cybercrimes Act 19 of 2020 in the Context of Civil Procedure: A Future Journey" 2020 *Obiter* 22.

45 Brar and Kumar "Cybercrimes: A Proposed Taxonomy and Challenges" 2018 *Journal of Computer Networks and Communications* 1–11.

46 *Ibid* 7.

47 *Ibid.*

48 *Ibid.*

49 *Ibid.*

50 *Ibid*.

51 *Ibid*.

52 *Ibid*.

> Cyberfrauds include social engineering attacks like guessing, spear phishing, and DNS re-directing in which the hacker manipulates the users to get their confidential information and then uses this information for his/her vested interests …[53]

Kumar defines cyberfraud as:

> The act of making financial or personal gain by deception is known as cyberfraud. The main aim of fraud is to gain benefits in terms of money. Cyberfrauds include social engineering attacks like password guessing, spear phishing, and DNS redirecting in which the hacker manipulates the users to get their confidential information and then uses this information for his/her vested interests …[54]

Kumar further argues that DNS re-direction is referring to "Domain Name Helper Service" which is a method that is used to serve "a web page to a user that is different from either the one requested or one that might reasonably be expected".[55] Brar and Kumar's averments above are significant in the interpretation and application of section 7 of the Act. This is because password attackers contravene the stipulations of section 7. When the consequences of these password attacks are invoked in civil proceedings, they constitute a cause of action that enables the plaintiff to institute civil proceedings against the defendant.

Broodryk argues that pleadings in practice must disclose a "cause of action".[56] He describes "cause of action" as meaning "every fact which is material to be proved in order to entitle a plaintiff to succeed".[57] This implies all the material facts that illustrate and confirm the damages that the plaintiff suffers because a contravention of section 7 by the defendant must be pleaded to enable the plaintiff to win. This may result in using the same cause of action that was used in criminal proceedings, if the defendant is convicted or sentenced for breaching section 7 of the Act.

Papadopoulos *et al.* argue that pharming hinders the protection of passwords because it happens "when victims are directed to fake bogus websites that trick them into supplying personal information such as credit card numbers and password".[58] Pharming is described as a method that:

> … can secretly redirect victims to a fraudulent website directly from their web browser. Pharming effectively eliminates the need for 'bait' emails and is therefore potentially more dangerous than 'normal' phishing scams and can cast a wider 'net' in which to snare victims …[59]

This pharming method may have dire financial consequences for the victims. These clients may lose substantial amounts of money, which they may not be able to recover. It appears that pharming is a gross violation of section 7 of the Act and the damages suffered because of such contravention confirm a cause of action that enables the plaintiff to institute civil proceedings

53 Brar and Kumar 2018 *Journal of Computer Network and Communications* 5.

54 *Ibid.*

55 http://www.techtarget.com (accessed 30-01-2023)

56 Broodryk (2019) *Eckard's Principles of Civil Procedure in the Magistrates' Court* (2019) 154.

57 *Ibid* 154–156

58 Papadopoulos *et al*. *Cyberlaw@SA* 480.

59 Upadhyay and Panchal "Unique Approach to Detect and Prevent Against Pharming Attack" 2019 *International Journal of Research and Analytical Reviews* 748.

against the defendant.

Brar and Kumar further state that snooping is another threat to the shield of passwords, particularly "digital snooping". They explain the term as follows:

> Digital snooping: Monitoring a private or public network for passwords or data is known as digital snooping. This attack is performed at the network layer. This snooping is done on the physical cable. Attackers may reprogram network switches or other devices to allow them to capture data off a network. Attackers can hack security cameras of an organization to get the username and password of employees so that they can access organization data like authorised users … [60]

When Brar and Kumar's above assertions are interpreted in the context of section 7 of the Act, they confirm that digital snooping adversely contravenes the provisions of section 7. Papadopoulos *et al.* argue that passwords protect "unauthorised access to or the unauthorised use of or interference with data, a computer program, a data storage medium or a computer system for criminal purpose".[61] Consequently, snooping accrues a cause of action when construed in the context of civil procedure and the plaintiff may institute civil proceedings when he/she suffers damages because of snooping.

These authors further indicate that phishing poses a threat to the provisions of section 7 because "phishing involves an email fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients".[62] This is done without acquiring a password from the plaintiff. When this is applied in the context of civil proceedings, the consequences of phishing that result in damages suffered by the plaintiff amount to a cause of action that enables the plaintiff to sue the defendant for such damages.

Neethling and Potgieter argue that it is imperative to ensure that the cause of action is well articulated when instituting civil proceedings.[63] They further assert, "a cause of action arises at the earliest date when all the requirements for delictual liability are present".[64] Resultantly, material facts should highlight evidence that confirms phishing right from the outset.

It is for this reason that I argue that the defendant who has been convicted and/or sentenced for breaching the stipulations of section 7 of the Act, should not be allowed to "get off scot-free" by raising a special plea.

3 THE IMPACT OF *RES JUDICATA* ON SECTION 7 OF THE CYBERCRIMES ACT

Res judicata is a defence that is used in civil proceedings through a special plea.[65] A special plea according to Pete *et al* is an objection raised to "knock out" the claim brought before the court.[66] This is done "before the merits of the plaintiff's case are even considered".[67] Authors such as Theophilopolos *et al* state that:

60 Brar and Kumar 2018 *Journal of Computer Network and Communications* 7.

61 Papadopoulos *et al. Cyberlaw@SA* 480.

62 Papadopoulos *et al. Cyberlaw@SA* 481.

63 Neethling and Potgieter *Law of Delict* (2020) 271.

64 *Ibid.*

65 Theophilopolos *et al. Fundamental Principles of Civil Procedure* (2020) 328; Broodryk *Eckard's Principles* 175.

66 Pete *et al. Civil Procedure: A Practical Guide* (2017) 203.

67 *Ibid*.

> *Res judicata* is an objection that the plaintiff's claim raises an issue that has already been dealt with and a final judgment pronounced thereon by another competent court, provided that the prior action between the same parties, concerning the same subject-matter, and founded on the same cause of action …[68]

The above authors are supported by Broodryk[69] and other authors.[70] I already made an argument in a previously published article that the time has come to relax the utilisation of *res judicata* in cybercrime matters.[71] I re-iterate that the courts should be flexible in the application res judicata.[72] The Supreme Court of Appeal in the case of *Democratic Alliance v Brummer*[73] further supports the argument that the application of the *res judicata* principle should be relaxed.[74] The cybercriminals should not get away easily because of the *res judicata* defence, because it will be an abuse of the court processes to use *res judicata* after the contravention of section 7 of the Act. Particularly, when there is evidence that confirms the plaintiff has indeed suffered a substantial financial loss because of a contravention of section 7 of the Act notwithstanding the fact that the defendants are already convicted or sentenced under the same provision.

4 INTERNATIONAL INSTRUMENTS REGULATING CYBERCRIMES

Before embarking on an analogy between the United Kingdom and South Africa, it is prudent to mention the significance of The Council of Europe's Convention on Cybercrime (Budapest Convention). The Budapest Convention regulates cybercrime on an international level and South Africa signed it. Chitimira and Ncube confirm that South Africa signed the Budapest Convention in 2001.[75] Mabunda argues that "according to the explanatory report to the Budapest Convention, the offence of illegal access covers basic threats to and against the security of a computer …"[76] It is argued that the Budapest Convention is important in civil proceedings.[77] I therefore assert that the relevant provision of the Budapest Convention that links with section 7 is Article 6. Article 6(1)(a)(ii) regulates passwords and access codes. Article 6(1)(b) is equally important and it includes the word "possession" of a password that is indicated in subsection (1)(a) of the Budapest Convention. Article 6(1)(b) is linked with the provisions of sections 4(1) and 7(1)(c) of the Cybercrimes Act. The incorporation of Article 6 into the provisions of sections 4(1) and 7(1)(b) is indicative of the fact that South Africa is truly committed to comply with the Budapest Convention.

5 AN ANOLOGY OF CYBERCRIMES IN THE UNITED KINGDOM

The provisions of the Fraud Act of 2006, the Criminal Justice Act of 2003, as well as the Electronic Communications Act of 2000 regulate cybercrimes in the United Kingdom. The stipulations of the Fraud Act of 2006 do not expressly incorporate a direct provision that is similar to section 7 of the Cybercrimes Act. However, section 7(1) of the Fraud Act of 2006

68 Theophilopolos *Principles of Civil Procedure* 328.

69 Broodryk *Eckard's Principles* 125.

70 Pete *Civil Procedure* 203.

71 Mabeka *International Journal of Law and Public Administration* 15.

72 *Ibid* 15.

73 Case no: 793/2021 2022 ZASCA (3 November 2022).

74 *Democratic Alliance v Brummer* Case no: 793/2021 2022 ZASCA (3 November 2022) para 12.

75 Chitimira and Ncube 2021 *PELJ* 5–6.

76 Mabunda (LLD-thesis, UWC, 2021) 72.

77 Mabeka and Cassim 2023 *Obiter* 31.

regulates fraud related offences, which include unlawful cybercrimes.[78] This was illustrated in the case of *Regina v Douglas*[79] where personal information such as passwords was hacked. The court considered the section 7 provision of the Fraud Act of 2006 and highlighted the significance of protecting personal information including passwords.[80]

Section 6 of the Electronic Communication Act of 2000 regulates "cryptography support service" in electronic data. This section states:

> … (1) In this Part "cryptography support service" means any service
>
> cryptography which is provided to the senders or recipients of electronic support services. communications, or to those storing electronic data, and is designed to facilitate the use of cryptographic techniques for the purpose of—
>
> (a) securing that such communications or data can be accessed, or
>
> can be put into an intelligible form, only by certain persons; or
>
> (b) securing that the authenticity or integrity of such
>
> communications or data is capable of being ascertained.
>
> (2) References in this Part to the provision of a cryptography support
>
> service do not include references to the supply of, or of any right to use, computer software or computer hardware except where the supply is integral to the provision of cryptography support services not consisting in such a supply ...

The construction of this provision denotes that the drafters intend to prevent the use of passwords for unlawful activities. This provision is akin to the stipulations of section 29 of the Electronic Communications and Transaction Act 25 of 2002 (ECT Act). It appears that the South African legislature had the same intention that is expressed in section 6 above.

It is apparent that both the United Kingdom and South Africa aim to protect data that is viewed as confidential in nature. Section 29(1) of the ECT Act places an obligation on the Director General to create and "maintain a register of cryptography provider". These cryptography providers are precluded from "disclosing confidential information".[81] It is evident that the legislature in South Africa had the same intention as the United Kingdom when it drafted section 29 of the ECT Act.

Another relevant provision is sections 1(3) and (4) of the Regulation and Investigatory Powers Act of 2016.[82] This provision is similar to sections 2 and 49 of RICA discussed earlier. They both aim to prevent interception that is conducted against the law. RIPA was promulgated to

78 The preamble of the Fraud Act of 2006; Section 7 relates to "Making or supplying articles for use in frauds". Section 7 states:
(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article— (a) knowing that it is designed or adapted for use in the course of or in connection with fraud, or (b) intending it to be used to commit, or assist in the commission of, fraud…

79 2019 EWCA Crim 95; 2019 WL 00691256.

80 *Regina v Douglas* 2019 EWCA Crim 95; 2019 WL 00691256.

81 Section 29(3) of the ECT Act.

82 Hereinafter referred to as RIPA.

regulate electronic communications and to prohibit unlawful interception. Section 1(3) states:

> … (3) These other protections include *offences and penalties* in relation to -
>
> (a) the *unlawful interception of communications*, and
>
> (b) the *unlawful obtaining of communications data*…

The construction of the above provision shows that it is the intention of the United Kingdom to prevent cybercriminals from obtaining data in a manner that is against the law. This provision can be linked with section 7 because the latter section also precludes people from acquiring or obtaining passwords and using data for activities or transactions that contravene the law. In addition, it appears that sections 2 and 3 of the Cybercrimes Act are also linked with section 1 of RIPA. This is illustrated by the use of words such as *offences* and *penalties*, which criminalise interception of data that is illegally conducted.

Subsection 4 of section 1 of RIPA enforces the provisions of subsection 3. This subsection states:

> … This Part also *abolishes* and restricts various general *powers to obtain communications data* and restricts the circumstances in which equipment interference, and certain requests about the interception of communications,can take place …

Similarly, subsections 3 and 4 of section 1 of RIPA prohibit a manner that allows cybercriminals to obtain computer or other devices' passwords, which are later used to commit cybercrimes. This is illustrated by the incorporation of the term "abolishes".

Further, phrases such as "powers to obtain communication data" demonstrate that the United Kingdom views unlawful interception that results from the use of a password contrary to the law, as a serious offence that warrants punishment. This is illustrated in the case of *Copland v The United Kingdom*,[83] where there was interception of an employee's electronic communication without her knowledge and without notification.[84] The interception was conducted after the employee visited another institution during her leave. The court considered the provisions of section 1 of RIPA. The court held that the interception should be more serious.[85] This implies that the use of passwords and interception thereof is very serious. The court held that:

> … In a number of cases relating to complaints involving the interception of their communications of suspected criminals by the police, in their view, a finding of violation should in itself constitute sufficient just satisfaction …[86]

In *Media Entertainment NV v Sapar Karyagdyyev, Alfonso Gonzalez Garcia*,[87] the claimant's business which is operated "online" was hacked.[88] Personal information was controlled by a password.[89] The court was of the view that there was sufficient evidence presented before the

83 2007 ECHR 253.

84 *Copland v The United Kingdom* 2007 ECHR 253.

85 *Ibid* 53–59.

86 *Ibid* 53.

87 2020 EWHC 1138 (QB); 2020 WL 02391006.

88 *Media Entertainment NV v Sapar Karyagdyyev, Alfonso Gonzalez Garcia* Case no: CL-2019 -000002.

89 *Ibid*.

court that proved that there was unlawful access to personal information.[90]

The court concluded that:

> … The Confidential Information in its very nature of Passwords to an entity's computer systems (as well as emails to and from third parties to the entity) is obviously both confidential in nature and not to be used without authorisation from that entity to access those systems and emails …[91]

Another similar case is that of *Rijksmuseum Twenthe v Simon C Dickinson Ltd*,[92] in which emails were hacked and funds were transferred into the hackers' accounts.[93] This was accomplished by sending spoof emails to the plaintiff. As a result, the plaintiff suffered damages. The court concluded that there was a duty on the defendant to verify the emails.

In *Warren v DSG Retail Ltd*,[94] there were cyber-attacks that resulted in the theft of confidential data: "the attackers infiltrated DSGs' system and installed malware which was running on Point 5930 of sale terminals at the stores".[95] Mr Warren's personal information such as date of birth and phone numbers were compromised, and he suffered damages.[96] It was argued that the infiltration that granted the cyber attackers access to personal information was a cause of action that warranted a civil claim.[97] The court was satisfied that there was indeed hacking which resulted in unlawful access to a customer's personal data and it concluded that the material facts of the case must be pleaded.[98] Consequently, the court held that there was a breach of duty to protect the personal data of customers.[99]

In *Smith v Talktalk Telecon Group Plc*,[100] personal data was accessed unlawfully and without permission.[101] The stolen data included information that relates to names, addresses and banking details. This data was used to commit fraud. It was argued that "the defendant was liable for failures which led to third parties obtaining unauthorised access to the relevant private information".[102] The court referred to the decision taken in the *Warren* case and confirmed that material facts must be pleaded to show the cause of action.[103] The court concluded that there was "unlawful accessing of the defendant's system".[104]

Subsection 4 of section 1 of RIPA may also be linked to section 7 of the Act because it prevents cybercriminals from obtaining passwords and subsequently using data to commit cybercrimes. This may be achieved by spoofing the emails of the plaintiff as seen in the case of *Rijksmuseum Twenthe*. Alternatively, the cybercriminals may hack the plaintiff's system as seen in the case

90 *Ibid*.

91 *Media Entertainment NV*, 21.

92 *Rijksmuseum Twenthe v Simon C Dickinson Ltd Media Entertainment NV v Sapar Karyagdyyev, Alfonso Gonzalez Garcia* Case no: CL-2019 -000002 (30 January 2020).

93 *Ibid*.

94 2021 EWHC 2168 (QB); 2022 E.C.C.9

95 *Warren v DSG Retail Ltd* 2021 EWHC 2168 (QB); 2022 E.C.C.9 para 1.

96 *Ibid* 14–16.

97 *Ibid* 16.

98 *Ibid* para 31.

99 *Ibid* para 41–43.

100 *Smith v Talktalk Telecom Group Plc* 2022 EWHC 1311 (QB); 2022 WL 01721252.

101 *Ibid* 7.

102 *Ibid* 3.

103 *Smith* 38.

104 *Ibid*.

of *Smith*.

The question is, can cybercriminals who are convicted and sentenced in terms of RIPA, raise a defence of *res judicata* when the plaintiff subsequently sues them for damages suffered because of a contravention of section 1? This question is answered with reference to the interpretation of the provisions of the Criminal Justice Act of 2003, particularly section 75. It is thus significant to construe the stipulations of section 75 of the Criminal Justice Act.

Section 75 of the Criminal Justice Act states:

> (1) This Part applies where a person *has been acquitted* of a qualifying offence in proceedings-
>
> (a) on indictment in England and Wales,
>
> (b) on appeal against a *conviction, verdict or finding* in proceedings on indictment in England and Wales, or
>
> (c) on appeal from a decision on such an appeal.
>
> (2) A person acquitted of an offence in proceedings mentioned in subsection (1) is treated for the purposes of that subsection as also acquitted of any qualifying offence of which he could have been *convicted in the proceedings* because of
>
> the first-mentioned offence being charged in the indictment, except an offence-
>
> (a) of which he has been *convicted*,
>
> (b) of which he has been *found not guilty* by reason of insanity, or
>
> (c) in respect of which, in proceedings where he has been found to be under a disability (as defined by section 4 of the Criminal Procedure (Insanity) Act 1964 (c. 84)), a finding has been made that he did the act or made the omission charged against him…

The construction of this section shows that the United Kingdom regards *res judicata* as a serious principle that deserves to be enforced. Further, section 75 indicates that even if the defendant had been found not guilty, the plaintiff may be faced with the dismissal of the case if the defendant raises *res judicata* as a special plea.

In the case of *Connelly v Director of Public Prosecution*,[105] the court had to determine whether the accused could be tried for the same matter on facts of law.[106] In coming to its conclusion, the court averred that the facts must accrue from the same cause of action to warrant for the defence of *res judicata* to be applied.[107] Further, the court held that the circumstances of the case determine whether the court should waive the application of *res judicata* when such court deems it necessary. The court further held that "the principle of *nemo debet bis vexasi* applies in criminal as well as civil cases".[108] It appears that the United Kingdom follows a flexible approach in applying the defence of *res judicata*.

Andrews asserts that no one should be tried twice for a matter that originates from the same course of action.[109] Further, the court should take certain factors into consideration when

105 1964 AC 1254.

106 *Connelly v Director of Public Prosecution* 1964 AC 1254, 1339.

107 *Ibid* 24.

108 *Ibid.*

109 Andrews *Court Proceedings, Arbitration & Mediation* (2019) 455–457.

deciding the application of *res judicata*.[110]

These factors are:

- There has been a decision in a civil matter (whether be a final decision, or a relevant type of consent order)
- That decision was made by a competent civil court or tribunal (including courts recognised under English rules of private international law and arbitration proceedings); and
- That decision was and remains valid and binding upon parties (and their privies or successors) …[111]

The application of Andrews' factors to section 7 of the Cybercrimes Act shows that the plaintiff may still institute civil proceedings against the defendant, if the defendant has not yet been convicted or sentenced. Ambrose *et al.* argue that the matter must be finalised by the courts in order to successfully raise a special plea on the grounds of *res judicata*.[112] Thus, as long as the matter has not been finalised, the plaintiff still has a chance of instituting civil proceedings against the defendant. Andrews further argues that there may be compelling circumstances that warrant a waiver in the application of a special plea based on *res judicata*.

Andrews supports his arguments by making reference to the case of *Virgin Atlantic Airways Limited v Zodiac Seats UK Limited*[113] where *res judicata* was raised as a special plea because the matter was already finalised in Technical Board of Appeal.[114] The court held that:

> … The plea of res judicata applies, except in special cases, not only to points upon which the court was actually required by the parties to form an opinion and pronounce a judgement, but to every point which properly belonged to the subject of litigation …[115]

The court further held that there must be special circumstances to warrant an exception on the application of *res judicata*.[116] This is further illustrated in the case of *Beedie v R*[117] where the court also said "special circumstances" compel courts to divert from employing the doctrine.[118] The court in *Regina v Z*[119] concurred with the decision of the court in *Connelly v Director of Public Prosecution*.

In *R v Weir*,[120] the accused was convicted twice for the same offence. The conviction was dismissed on appeal. Subsequently, there was new and reliable evidence that called for a waiver of the application of *res judicata*.[121] The court concluded that "new compelling, reliable and

110 *Ibid*.

111 *Ibid* 455.

112 Ambrose *et al. Blackstone's Civil Practice* (2021) 83.

113 2009 EWCA Civ 1062; 2013 UKSC 46.

114 *Virgin Atlantic Airways Limited v Zodiac Seats UK Limited* 2009 EWCA Civ 1062; 2013 UKSC 46 (hereinafter *The Virgin* case).

115 *Ibid* 18.

116 *Ibid* 38.

117 1997 EWCA Crim 714.

118 *Beedie v R* 1997 EWCA Crim 714, 5, 6 and 8.

119 On Appeal from The Court of Appeal Criminal Division 2000.

120 2005 EWCA Crim 2866.

121 *R v Weir* 2005 EWCA Crim 2866, 55 (*The Weir* case).

substantial evidence" forced the court to waive the consideration of the doctrine.[122]

When this decision is applied in light of section 7 of the Act, it means that the plaintiff may present new evidence that arises from the same cause of action that was not used in the criminal court. It is argued that *res judicata* should be waived when the defendant is convicted of contravening section 7 of the Act, where the plaintiff produces new evidence of the profits gained by the defendant from the contravention of section 7.

In *Spire Healthcare Limited Claim v Nicholas Brooke*, Mr Jellet brought a claim for damages for personal injuries that he suffered.[123] He had gone for an operation but there were complications. He suffered internal bleeding which led to tetraplegia. There was an agreement signed, which became a consent order. Mr Jellet complained again and argued that there was a new cause of action and new allegations that were not raised before the agreement was signed. Mr Brooke tacitly raised double jeopardy. The court held that the agreement completed the finality of the matter because the new allegation accrued from the same cause of action that was covered in the agreement. Had the new allegation arose from a cause of action that was outside the terms and conditions of the agreement, the court would have decided otherwise. The court concluded that:

> Whilst some of the allegations now made may be more details, and the emphasis may have, in part, changed, in my judgment, these differences do not amount to the raising of new "issues" which were not raised in the original proceedings…[124]

This decision is raising an exception to the strict application of the doctrine of double jeopardy, and it enables plaintiffs to institute civil proceedings against the defendants who are facing criminal charges or are convicted or sentenced for contravening section 1 of RIPA. This case is relevant because, if there are new allegations that were not dealt with by the court when the defendant was convicted and sentenced for contravening section 1 of RIPA, the plaintiff may successfully sue the defendant.

It appears that the United Kingdom courts follow a similar approach that holds the defendants accountable for the damages suffered by the plaintiffs, which stem from hacking or unlawful interception. This is seen in cases such as *Global & Local Investment* , *Fourie*, *Geber, Hartog* and so forth, in South Africa. In the UK, the cases that show a similar approach are cases such as *Smith*. However, the Supreme Court of Appeal recently followed another approach in *Edward Nathan Sonneberg Inc*. It refused to endorse the decision to award damages to the plaintiff because the latter had sufficiently been warned about cybercrime by ENS. This is the only exception so far; it remains to be seen whether the constitutional court will follow the Supreme Court of Appeal approach in the future.

Brown *et al.* affirm that *res judicata* is raised as a special plea[125] And further, that in civil proceedings the plaintiff may use *res judicata*, which is a defence intertwined with the doctrine of double jeopardy in accordance with Roman-Dutch Law.[126] Brown *et al.* argue that *res judicata* enforces the finality principle but this should be waived when special circumstances warrant the waiver.[127] Stuckenberg asserts that when there is new compelling evidence after the acquittal or conviction, the courts should do away with the *res judicata* and allow the plaintiff to institute

122 *Ibid*.

123 2016 EWHC 2828.

124 *Spire Healthcare Limited Claim v Nicholas Brooke* 2016 EWHC 2828 at 123.

125 Brown, Turner and Weisser *The Oxford Handbook of Criminal Process* (2019) 457–475.

126 *Ibid* 458.

127 *Ibid*.

civil proceedings.[128] Stuckenberg further narrows down the meaning of the same cause of action as, "the same facts" or "same act or omission"; "same conduct" and "same transaction".[129]

Furthermore, the cause of action can also be construed as "same evidence" and "same statute".[130] When these descriptions of a cause of action are interpreted in terms of section 7 of the Act, it means the plaintiff will not have recourse. This is a narrow interpretation of the descriptions. However, the contextual interpretation of the description warrants a waiver when the circumstances call for such a departure. The same facts refer to *facto probanda* and *facto probantia*.[131] These "same facts" must be pleaded to show and confirm a cause of action.

The courts should not entertain the special plea raised by the defendant based on *res judicata*. This is usually the case where there are proceeds that are established from a contravention of section 7. Although it may be argued that the proceeds accrue from the same cause of action, the establishment of these after conviction confirms that this is new evidence that forces the courts to waive the application of *res judicata*.

6 FACTORS TO CONSIDER IN CIVIL PROCEEDINGS WHEN WAIVING THE APPLICATION OF *RES JUDICATA* IN THE CONTEXT OF SECTION 7 OF THE ACT

First, the court must determine whether the unlawful acquisition or possession of the password was due to the negligence of the plaintiff. For example, if the plaintiff wrote the password on a piece of paper and left it on his desk knowingly, someone may access the password but has a reasonable and justifiable explanation why he left the password on the desk. It is significant to observe that authors such as Theophilopolos agree that encryption or password protection is important in practice. He asserts that:

> The document is encrypted using a software cryptographic algorithm which contains a lengthy and randomly selected set of binary digits, described as a binary key. In most instances the same binary key may be used to encrypt and decrypt the document, but it is also possible to use different binary keys for the purpose of encryption and decryption. Further, the longer the binary key (some types of encryption software allow for binary keys of hundreds of decimal digits), the more difficult it is to break the encryption …[132]

The averments of Theophilopolos supports the first factor. Thus, the plaintiffs should ensure that passwords are not written on paper and are not at risk of being accessed by those who are around them.

Further, Papadopoulos *et al*. confirm that it is imperative to shield electronic data by using passwords.[133] This is why the courts should award fewer damages because the unlawful acquisition of the password has dire consequences in practice, particularly in the application of the privilege principle that legal practitioners should adhere to. Clients' confidential information that is viewed as privileged may be accessed.

Second, the courts must look at the extent of the damages suffered by the plaintiff to waive the application of the doctrine. For example, if there is compelling evidence presented in the court that proves that the plaintiff suffered a substantial amount of damages because of a contravention

128 Stuckenberg "Double Jeopardy and *Ne Bis in Idem* in Common Law and Civil Law Jurisdictions" in Brown et al. *The Oxford Handbook of Criminal Process* (2019) 457–475.

129 *Ibid* 466.

130 *Ibid*.

131 Broodryk *Eckard's Principles* 27.

132 Theophilopolos *et al Principles of Civil Procedure* 599.

133 Papadopoulos *et al. Cyberlaw@SA* 480.

of section 7, the court should waive the application of *res judicata*. The plaintiff in the *Fourie* case suffered damages for an amount of 1 744 599.45 "(one million seven hundred and forty four thousand and five hundred ninety rand and forty five cents)"[134] and in the *Hartog* case the plaintiff suffered damages for an amount of 1 421 228.06.[135] This substantial amount deserves to be returned to the plaintiff who suffered damages arising from a contravention of section 7 of the Cybercrimes Act.

Third, the courts must consider whether the defendant was asked by the court to pay compensation to the plaintiff in criminal proceedings as a sanction where evidence was presented that confirms a substantial amount of damages suffered by the plaintiff. If not, the courts should consider waiving the application of *res judicata* and allow the plaintiff to recover the damages through civil proceedings.

Finally, the question whether the defendant has already appeared in trial proceedings or is just beingcharged for contravening section 7 of the Act should be raised. If the defendant has not yet appeared in court when the plaintiff institutes civil proceedings, the courts should waive the application of the doctrine of double jeopardy.

7 CONCLUSION

There is no doubt that the legislature intended to prevent *unlawful acquisition* and *possession* of passwords when it enacted section 7 of the Act. It is significant to affirm that the consequences of a contravention of this provision amount to a cause of action that enables the plaintiff to institute civil proceedings against the defendant. This is seen from case law that awards damages suffered from an unlawful interception such as *Fourie*, *Global & Local Investment*, *Hartog* and so forth. However, it is observed that, when the plaintiff sues, the defendant may raise a special plea on the grounds of *res judicata*.

Thus, the analysis of the provisions of section 7 of the Act, as well as the examination of *res judicata* demonstrate that there is a need to waive the application of the latter in civil proceedings that arise from a contravention of this stipulation. It is submitted that the factors highlighted in this article, should be used by the courts in instances where the plaintiff institutes civil proceedings against the defendant based on the same cause of action that originates from the consequences of a contravention of section 7 of the Act.

The United Kingdom follows the same flexible approach as South Africa when deciding whether to waive the application of *res judicata*. This is observed from the decisions in cases such as *Media Entertainment NV*, *Rijksmuseum Twenthe*, *Warren*, and *Smith*. The United Kingdom courts are also flexible and this is illustrated in the decision of the court in the case of *R v Weir*. The authors such as Andrews and Ambrose *et al* in the United Kingdom support the flexible approach. Andrews[136] goes further and provides factors to be considered when courts waive the application of *res judicata*. I suggest that South African courts should carefully apply their minds and waive the application of *res judicata* when there is a civil claim that stems from the consequences of a contravention of section 7 of the Act. Lastly, the author submits that the consequences of a contravention of section 7 constitute a cause of action when applied in civil procedure and this is indeed an incredible journey to success.

134 *Fourie* para 9.

135 *Hartog* para 12.

136 Andrews *Court Proceedings* 455.