RedFame

International Journal of Law and Public Administration
Vol. 5, No. 2; December 2022
ISSN 2576-2192 E-ISSN 2576-2184
Published by Redfame Publishing
URL: http://ijlpa.redfame.com

The Application of Section 8 of Cybercrimes Act 19 of 2020 in Civil Procedure in South Africa is a Hailing Snow: A Comparative Studies between South Africa and United Kingdom

Nombulelo Queen Mabeka

College of Law, University of South Africa. South Africa.

Received: November 18, 2021 Accepted: December 8, 2021 Online Published: December 7, 2022

doi:10.11114/ijlpa.v5i2.5814 URL: https://doi.org/10.11114/ijlpa.v5i2.5814

Abstract

In South Africa the legislature passed a statute that regulates cyber fraud that is called Cybercrimes Act 19 of 2020 in an attempt to combat cybercrimes, which include cyber fraud. The commission of cyber fraud in Civil Procedure constitutes a cause of action that enables the victim to claim for damages. It is not clear in terms of Cybercrimes Act whether the victim may institute proceedings whilst the matter is pending before the court in criminal proceedings or after the perpetrator is convicted. This raises a question on the application of the two common law principles that the defendant may raise as a special plea. Thus, *res judicata* and *lis pendens* may be raised as a special plea to prevent the victim of cyber fraud from receiving compensation for damages suffered. This prejudices the victims because some of the consequences that result from cyber fraud are dire to the victim. For example, the victim may loose money, property and may psychologically be affected as a result of cyber fraud. This article follows a qualitative research methodology that is based on an analysis in jurisprudence. Thus, the article looks at section 8 of the Cybercrimes Act, judicial precedent, as well as scholarly views shared by various authors to determine the gap. The author provides a solution, as well as recommendations that will ensure that the victims have a recourse in Civil Procedure. Moreover, there is evidence that proves that cyber fraud does exist in jurisdictions such as the United Kingdom. The article examines the legal position of cyber fraud in the United Kingdom and does a comparative studies between South Africa and the United Kingdom.

Keywords: Cyber fraud, Section 8 of Cybercrimes Act, Civil Procedure, cause of action, *lis pendens*, *res judicata*, United Kingdom, special pleas

1. Introduction

Cybercrime is becoming a major concern these days because victims are hacked and their information is used to commit cybercrimes. The South African legislature recently passed Cybercrimes Act 19 of 2020 to combat cybercrimes. This is a very good attempt because cybercriminals are dealt with accordingly.

It is observed however that the legislature omitted to include the direct application of the Cybercrimes Act in civil proceedings yet cybercrime constitutes a cause of action that enables the plaintiff to institute civil proceedings against cyber criminals. This article uses a qualitative research methodology that is based on the interpretation of the relevant provisions of sections 8 of the Cybercrimes Act to determine the gap and the extent thereof. In addition, the article discusses the position of cyber fraud in the United Kingdom and the reason why this jurisdiction is chosen based on the fact that the British legal system influenced South African legal system. Further there is compelling evidence that shows that cyber fraud does exist in the United Kingdom regardless of the water tight laws that are in place. This is followed by a comparative studies between South Africa and the United Kingdom. The article concludes by providing a cure to the gaps that are identified

2. The Interpretation of Section 8 of Cybercrimes Act 19 of 2020

The preamble of the Cybercrimes Act confirms that it was passed to regulate cybercrimes. This Act makes it an offence to unlawfully intercept electronic communications. Further, it is an offence to tamper with electronic communications and use the same to commit fraudulent activities. The Act also prohibits the disclosure of information which may be viewed as hurtful. A section of a legal instrument comprises of several provisions and is not one provision itself.

Section 8 states that:

> …Any person who *unlawfully* and with the *intention* to defraud makes a Misrepresentation-
>
> *(a)* by means of data or a computer program; or
>
> *(b)* through any interference with data or a computer program as contemplated in section 5(2)*(a)*, *(b)* or *(e)* or interference with a computer data storage medium or a computer system as contemplated in section 6(2)*(a)*, which *causes actual or potential prejudice to another person*, is guilty of the offence of cyber fraud…

The key aspects of this stipulation is that an act or omission must be *unlawful, intentional* or it must have been conducted without the permission of the victim or the plaintiff. Secondly, there must be a *misrepresentation* done through cyber fraud, which *prejudices* the victim. The further construction of this provision demonstrates that it is the intention of the legislature to prohibit cyber fraud. The inclusion of the word 'intention' in this provision is indicative of the fact that the legislature views cybercrime as a very serious offence that deserves to be punished in law. The law shows that cyber fraud happens more often than not in cases where the plaintiff's personal or confidential information is hacked by cyber criminals and used to commit fraud. This is usually the case in the banking industry where the perpetrators get someone who works in the bank to hack clients' information and use it for fraud as seen in the case of *Msomi v S* 2020 1 SACR 197 (ECG). In this case the syndicate was charged with fraud in accordance with the provisions of section 86 of the Electronic Communications and Transactions Act 25 of 2002, which was repealed by Cybercrimes Act in 2020.

It was argued that the appellant unlawfully extracted 'computer software' of the bank and later conducted unlawful transactions. The court highlighted the fact that hackers indeed unlawfully gained access to computers and utilized the information for their own benefits. Consequently, the court awarded the harshest sentence of imprisonment because it demonstrated intolerance in cybercrime.

Cassim (2011) argues that cyber fraud is a matter of concern. Cassim (2009) asserts that the United Kingdom is abreast with the implementation of measures that seek to combat cyber fraud as compared to South Africa. Snail (2009) supports Cassim in her averment that cybercrime is becoming a problem in South Africa (Snail, 2009, p.1-13).

In another recent decision, the court put emphasis on the fact that some plaintiffs are implicated into cyber fraud by hackers and this prejudices them in an adverse manner. This was illustrated in the case of *Fouries v Van der Spuy and De Jongh Inc. and Others* 2020 1 SA 560 (GP). This is a case of attorneys who were custodians of clients' money that was in the trust account. A lucrative amount was used to make payments to hackers based on instructions they gave to the attorneys under pretence. It became apparent that the client did not give such instructions and asked the court to grant an order for the payment made without the knowledge of the latter. The court decided in favour of the client because the attorneys' were supposed to take stringent measures to protect clients' money from hackers by verifying the instructions.

The *Fourie* case is a classic example of civil litigation where evidence shows that the cause of action arose from cyber fraud. This is said because the emails that the hackers sent to the attorneys instructing them to conduct unlawful transactions whilst pretending to be a client, amounted to a cause of action. This is why the plaintiff was successfully awarded the amount that cyber fraudsters claimed from the attorneys. It is argued that cybercrime on its own constitutes a cause of action, which enables the victim to institute civil litigation or proceedings for defamation of character as seen in the case of *Fourie;* although it does not deal with defamation *per se*, it actually deals with a cause of action that arose from cyber fraud. Pete *et al* (2017) also aver that the main basis of the cause of action is the complaint that is brought before the court. Further, the elements of facts presented by the client to the legal practitioner, which the legal practitioner will prove in court, constitute a cause of action (Pete *et al*, 2017, p. 24). Broodryk (2019) argues that the cause of action determines the appropriate remedy sought by the plaintiff. Thus, a client may receive money based on the type of the claim that is brought before the court (Broodryk, 2019, p. 6). It is submitted that the claim in the instance of this article is cyber fraud.

The questions that has not yet been answered by the courts because the Act is new is whether or not the victims may simultaneously claim for damages whilst the matter relating to the same cause of action is pending before the court. It is borne in mind that cyber fraud that implicates innocent individuals infringes on such individuals' right to dignity and also privacy because the disclosure of personal or confidential information falls within the ambit of the law of privacy. Neethling & Potgieter (2021) argue that the cause of action is illustrated by the presence of *fact probanda* (Neethling & Potgieter, (2021), p. 271). These authors assert that the commission of fraud enables the plaintiff or the victim to claim damages (Neethling & Potgieter, (2021), p. 284). Van der Merwe et al. (2016) affirm that the courts accept that fraud committed by means of electronic communications falls within the ambit of cyber fraud (Van der Merwe et al., 2016, p.74) .

Undoubtedly those whose rights have been violated may ask the court to grant compensation in terms of section 38 of

the Constitution of the Republic of South Africa. However, there is still a gap in Cybercrimes Act that must be addressed to allow victims to institute proceedings concurrently.

This is due to the fact that criminal proceedings take a long time to be finalized and by the time a case finalized, the victim may be penniless. Instituting a civil claim at the same time as a criminal matter allows the defendant and/or legal practitioners to settle for a specific amount to satisfy the loss suffered by the plaintiff.

It is submitted that the simultaneous proceedings will satisfy the victim for the loss suffered and it will stop the behaviour in a way. This shows that there is a need to relax the application of *lis pendens* and *res judicata* in cybercrime matters to overcome cyberattacks. It appears that the times has come to consider changing our law regarding these two principles. It is submitted that the relaxation of the application of these principles must only be employed in cybercrimes, particularly in section 8 matters to avoid confusion and overwhelming the courts. Cyber fraud is more damaging to the victims than any other cybercrimes because they may loose money they invested for decades and this may have dire consequences. If the plaintiff sues through civil litigation, the defendant may raise *lis pendens* as a defence. Pete et al. (2017) assert that the element of *lis pendens* is that you cannot institute a claim arising from the same cause of action, which is pending in another court (Pete *et al.*, 2017, p.212). These authors aver that the test that determines the application of *lis pendens* in civil procedure is based on an assessment of the pleadings (Pete *et al.*, 2017, p. 212). It is submitted that there is a gap in the Act Cybercrimes that the legislature must consider to close because the principle of *lis pendens* has been applied in many decisions and the courts strictly apply it when the matter which relates to the same cause of action is pending before the court.

In the case of *Socratous v Grindstone Investments* 2011 6 SA 325 (SCA), the Supreme Court of Appeal affirmed that *lis pendens* is applied when there is 'litigation pending on the same matter' that is similar to the case. In another case, *Hassen v Berrage* the court held that 'Fundamental to the plea of *lis pendens* is the requirement that the same plaintiff has instituted action against the same defendant for the same thing arising out of the same cause'. This was later enforced by the constitutional court in subsequent decisions. More often than not, the courts tend to link *lis pendens* with *res judicata*. Pete *et al* profess that *lis pendens* and *res judicata* are intertwined and inseparable (Pete et al, 2017, p.212). This is well illustrated in *Ceasorstone Sdot-Yam Ltd v The World of Marble and Granite* CC (741/12) 2013 ZASCA 129 (26 September 2013). The court held that the first matter must be finalized before another civil litigation may be ensued, which relates to the same matter. According to the court, the finality is important because *res judicata* is 'directed at achieving the same policy goals'. Meaning that the court must award a remedy that will satisfy the loss caused by cyber fraud and this is accomplished by sentences that are provided in the provisions of Cybercrimes Act.

Thus, the court compensates the victim or the plaintiff for the loss or damage resulting from cyber fraud. The court acknowledged the application of *res judicata* principle in as far back as Voet's period. It is evident that the promulgation of Cybercrimes Act is crucial in civil procedure because cybercrimes committed in contravention of section 8 raise a cause of action although there are no provisions that are incorporated into the Act that deal with the latter.

3. The Position of Cyber Fraud in the United Kingdom

The legal position of the United Kingdom is pertinent in South African Law because it has influenced the latter courts to develop the law to be in line with the principle of *boni mores*. This is why the United Kingdom is chosen as a comparative studies in this article. Unlike South Africa, cyber fraud is not expressly regulated in the United Kingdom statutes. The provisions of the Computer Misuse Act of 1990 tacitly regulate the modification of data without permission. Section 3 of the said Act makes it an offence to alter computer information without permission. In addition section 3(2) asserts that there must be an intention to change the data for a person to be held accountable. There is no direct provision of cyber fraud; its regulation is inferred in the provisions of sections 1 to 3 because they prohibit unlawful interception of data. The analogy of the provisions of Data Protection Act of 2018 shows that this Act regulates the processing of electronic communications. This Act precludes unlawful processing of data without consent. Suffice it to say that one may draw an inference that cyber fraud is strictly prohibited when processing personal information in terms of the provisions of the Cybercrimes Act. Section 4 of the Communications Act of 2000 precludes the disclosure of personal information without consent. There are however few exceptions, thus a disclosure done in relation to litigation is permitted in terms of section 4(2)(e) of the Communications Act.

The most relevant statute in the United Kingdom that specifically deals with fraud or cyber fraud is the Fraud Act of 2006. This is more applicable in cyber fraud because this Act articulates and narrows down the meaning of fraud in sections 2, 3 and 4 of the Fraud Act. Section 2 indicates that false representation falls within the ambit of fraud. It is significant to interpret the provisions of section 2 because the latter shows the link between section 8 of the South African Cybercrimes Act and section 2 of the Fraud Act of 2006.

Section 2 states:

(1) A person is in breach of this section if he—

(a) *dishonestly makes a false representation, and*

(b) intends, by making the representation—

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss.

(2) A representation is false if—

(a) it is untrue or misleading, and

(b) the person making it knows that it is, or might be, untrue or misleading.

(3) "Representation" means any representation as to fact or law, including a representation as to the state of mind of—

(a) the person making the representation, or

(b) any other person.

(4) A representation may be express or implied.

(5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to *any system or device designed to receive, convey or respond to communications* (with or without human intervention)

The construction of section 2(1) illustrates that cyber fraud committed by a cybercriminal who dishonestly uses a victim's electronic signature with the intention to commit fraud, prejudices the victims because he or she suffers financial consequences as a result of such cyber fraud. For example, the electronic signature may be used to purchase goods that are delivered to a fictitious address and the victim's name may later be listed as a bad payer, if the amount for such goods is not paid in full. It is important to observe that section 2(5) recognises the use of devices which may include the use of computers to commit cyber fraud.

The application of the provisions of section 2 of the Fraud Act is seen in the case of *R v Ghosh* 1982 EWCA Crim 2, where the court highlighted the dishonesty test that is incorporated into section 2(1) of the Fraud Act. The court held that the dishonesty test must be based on the 'objective test'. This principle was later applied and enforced in the case of *Ivey v Genting Casinos UK Ltd t/a Crockford* 2017 UKSC 67. In the said case, the court narrowed down the meaning of dishonesty in fraud related cases and described dishonesty as one of various types of fraud. In addition, the court stipulated that:

> …A significant refinement to the test for dishonesty was introduced by *R v Ghosh* [1982] QB 1053. Since then, in criminal cases, the judge has been required to direct the jury, if the point arises, to apply a two-stage test. Firstly, it must ask whether in its judgment the conduct complained of was dishonest by the lay objective standards of ordinary reasonable and honest people. If the answer is no, that disposes of the case in favour of the defendant. But if the answer is yes, it must ask, secondly, whether the defendant must have realised that ordinary honest people would so regard his behaviour, and he is to be convicted only if the answer to that second question is yes…

Suffice it to say that the two stage inquiry test should also be applied in cyber fraud because cyber criminals are dishonest when they unlawfully intercept the victims' computers and use the latter's information for personal gain. Further, when cyber criminals hack computers to gain access to personal information such as bank accounts, they know that 'ordinary' and 'honest' persons work hard to earn their living and they do not hack people's devices to obtain information that will be used to commit cyber fraud. There is no doubt that the provisions of section 2 regulate cyber fraud in the United Kingdom just as it is the case in section 8 of Cybercrimes Act.

Other provisions of the Fraud Act that deserve to be mentioned are sections 4, 7 and 11 respectively. Section 4 illustrates that abuse of position also constitutes fraud. Section 7 is equally important because it deals with articles that are supplied for the purpose of committing fraud. This is usually the case in academics and the victims may successfully institute civil proceedings against the perpetrators. Just as it is the case in section 2, section 7 also requires the presence of an intention to commit the crime. Section 8 describes the word 'article' as referring to 'data' or electronic communications. This happens when academics computers are hacked and their articles or data that are unlawfully intercepted and later used to commit cyber fraud for personal gain. Some of the hackers get money or compensation

from other perpetrators for breaching section 7 of Fraud Act.

Section 11 of the Fraud Act of 2006 makes it an offence to 'obtain services for himself or another by a dishonest act'. Once again this section is relevant in data that is unlawfully obtained from cyber space and subsequently used to commit cyber fraud. This usually occurs when a person's qualifications are unlawfully obtained in cyber space and later on adjusted to include the cyber fraudster's personal details who uses them to get a senior position that has high income. This amounts to cyber fraud and the victim when he/she becomes aware of the cyber fraud, may institute civil proceedings against the perpetrators.

It is significant to illustrate that businesses may be held vicariously accountable when there is evidence showing that cyber fraud was committed by those they are connected to. For example, in the case of *WM Morrisson Supermarkets PLC v Various Claimants* 2020 UKSC 12, the employee (Skeleton) who was employed by WM Morrison Supermarkets committed cyber fraud. Skeleton worked in payroll and he disclosed personal and confidential information on the internet. The court applied the close connection test to determine vicarious liability. The court held that although Skeleton worked in payroll, he was a data controller who could be viewed as a person that is closely connected to WM Morrison. This case is discussed because it shows that when a colleagues hacks another colleagues' computer and unlawfully obtains the latter's electronic signature; and subsequently commit cyber fraud by using such signature, the victim may institute a claim for damages against the colleague, as well as the employer because the cause of action arose based on the use of the employer's computer. Further the closer connection test will be satisfied when there is evidence that shows the colleague indeed hacked the computer. The victim may be granted compensation as a result of such cyber fraud.

It is submitted that section 2 particularly subsection 1 is similar to the stipulations in section 8 of the South African Cybercrime Act of 2020. Both provisions highlight the word(s) *dishonesty* or *misrepresentation* and the *intention* to commit fraud. The same applies for others sections that are mentioned above, namely, section 7 and 11, they all seek to prevent cyber fraud. According to Whitty (2019) cyber fraudsters target those who invoke digital technology (Whitty, 2019, p. 277). Further, there is evidence that shows that cyber fraud does exist in the United Kingdom (Whitty, 2019, p. 278). In some instances, individuals were tricked by cyber fraudsters and later suffer financially because the cyber criminals take their money after tricking the victims (Whitty, 2019, p. 281).

The question is, can the said victim sue the perpetrators after they are convicted in terms of the Fraud Act? Secondly, if they can do so, does the defendant or perpetrator has a right to raise a special plea based on *res judicata*? Another question is, can the plaintiff sue the defendant whilst the matter is dealt with in terms of the Fraud Act? If so, can the defendant raise special plea based on *lis alibi pendens* principle? It is important to observe that the Fraud Act does not incorporate a stipulation that allows the plaintiff who is a victim of cyber fraud to institute civil proceedings whilst the perpetrators is subjected to criminal proceedings based on the same cause of action.

The court in *Catalyst Investment Group Ltd v Lewinsohn and Others* 2009 EWHC 1964 (Ch) had to consider the employment of *lis alibi pendens*. It was argued that the courts must be more flexible in the application of the principle *lis alibi pendens* as opposed to a strict approach.

The author concurs with the flexibility approach because when the courts apply the principle in cyber fraud, this becomes critical to the plaintiffs who are victims of cyber fraud and who had suffered financially and otherwise as result of such cyber fraud.

These victims deserve to be awarded compensation in civil litigation even if the matter is still pending before another court. This will enable them to acquire satisfaction and recover from the loss suffered. With that said, it is the view of the author that the victims should not be deprived of their right to be awarded compensation by the civil courts because the matter relating to the same cause of action is pending before another court. It is submitted that the United Kingdom should consider doing away with the principle in cases where there is evidence that proves financial and emotional loss resulting from cyber fraud. Thus, the courts should use their discretion and allow parties to present the evidence that proves damages, before the courts dismiss the matter based on *lis alibi pendens*.

In as far as *res judicata* is concerned, the United Kingdom has applied this principle in 1843 in the case of *Henderson v Henderson* (1843-60) All E.R Rep.378. In the case of *Virgin Altantic Airways Ltd v Zodiac Seats UK Limited* 2013 UKSC 46, the court set out six principles of *res judicata* one of which is applicable to cyber fraud. The first principle is that when *facta probanda* is present in a matter, the parties may not institute further proceedings when the outcome is determined. Furthermore, when the plaintiff received compensation for damages in the first proceedings and such decision is not appealed, the plaintiff may not institute further proceedings based on the same *facta probanda*.

In addition, where the judgment is delivered by the court on a cause of action, a further claim will be regarded as nullified. The fourth principle relates to the binding effect in situations where common issues were finalized in a cause

of action that is not necessarily the same as the matter before the court. This means that parties in such instances may not institute further proceedings because they are bound by the decision taken in a judgment that has common issues. The next principle stops parties from instituting another action that could have been raised in an earlier matter. The last principle prevents parties from abusing the procedures and this is viewed as a matter of policy but it is not applied in the 'doctrine of merger. Ambrose et al. (2021) indicate that *res judicata* is significant to stop parties from repeating civil proceedings. The same authors asset that litigants may not bring a matter before the court that has already been decided upon based on the principle of *res judicata* (Ambrose et., 2021, p. 83).

The analysis of the above six principles demonstrates that the first and second the principles are more applicable in cyber fraud. It is evident that when one looks at the first principle, the victim who wishes to institute a claim for damages in terms of civil procedure may not do so after the defendant who is the accused in the criminal proceedings is convicted and sentenced in accordance with the Fraud Act. It is argued that the time has come to review this principle and consider doing away with the application of the principle in cases where there is compelling evidence that proves substantial damages that are presented in a form of patrimonial or non-patrimonial loss suffered by the victim as a result of cyber fraud.

It is argued that the courts should be allowed to award compensation to the victims in these instances regardless of the conviction and/or sentencing in terms of the Fraud Act of 2006.

Furthermore, the second principle may also be raised by the defendant when he has already been convicted. This implies that when the perpetrators are already convicted and sentenced, the sentencing was not challenged, the claimant may not later sue for damages based on the same cause of action. It is argued that this principle limits the plaintiff who has suffered severe damages as a result of cyber fraud committed by the perpetrator. For example, where the perpetrator used the victim's electronic signature to open fictitious companies, which were subsequently liquidated, and the creditors claim the monies due and payable from the plaintiff whilst such plaintiff is innocent, the second principle of the *res judicata* should not be applied. The courts in such instances should consider attaching assets of the defendant or award compensation to the innocent plaintiff.

Authors such as Andrews (2019) argues that *res judicata* is a matter of public policy and he affirms that the *Virgin Atlantic* case is a benchmark in the application of *res judicata* Andrews (Andrews, 2019, p. 455-461). Andrews further asserts that the application of *res judicata* in civil matters shields the rights of the parties to the proceedings (Andrews, 2019, p. 460). Moreover, the principle functions well for both the plaintiff and the defendant (Andrews, 2019, p. 460).

4. A Succinct Comparative Studies between South Africa and United Kingdom

It is observed that both jurisdictions seek to prevent cyber fraud in different statutes such as Fraud Act of 2006 in the United Kingdom and Cybercrimes Act of 2020 in South Africa. Both statutes incorporate *dishonesty* and *intention* to commit cyber fraud or fraud in different terms. For example, section 8 of the Cybercrimes Act infers the word *dishonesty* through the use of the word *misrepresentation* whilst the stipulations of the Fraud Act expressly refer to dishonesty. The constructions of both these statutes demonstrates that they all work towards achieving one goal, namely to regulate cyber fraud or fraud.

It is also observed that both these statutes do not incorporate a provision that allows parties to simultaneously institute civil proceedings against the perpetrators who are facing criminal charges or convicted of the same cause of action. This may be the case because of the application of the two common law principles, namely, *res judicata* and *lis alibi pendens*. It is submitted that the time has come to review and reconsider the application of these principles in cases of cyber fraud where the victims has suffered severe patrimonial and non-patrimonial loss. This implies that the courts should be allowed to use their discretion to hear matters, which the cause of action arose from cyber fraud, without concerning themselves about the application of these principles.

It is submitted that section 8 of the Cybercrimes Act of 2020 should incorporate a provision which enables parties to institute civil proceedings before or after conviction of the perpetrator in order to enable the victim to receive satisfaction.

The amendments should also incorporate a stipulation that relaxes the application of *res judicata* and *lis alibi pendens*, which the defendant or the perpetrator may use as a special plea. In as far as the Fraud Act of 2006 is concerned, the tacit recognition and regulation of cyber fraud in section 2 should be expanded on just as it is the case in section 8 of the Cyber Fraud.

5. Conclusion

There is no doubt that South Africa has a very good stipulation that articulates the regulation of cyber fraud in Cybercrimes Act. However, it is evident that the actual act of cyber fraud, which raises a cause of action that

enables the victim to institute civil proceedings is not included in the provisions of section 8 of the Cybercrimes Act. It is evident the defendant may raise a special plea when the plaintiff who instituted criminal charges against the defendant and subsequently sue in terms of civil procedure. Thus, the courts may be forced to dismiss a claim for damages arising out of cyber fraud when the defendant uses *lis pendens* or *res judicata* as a defence in civil litigation. This is a major problem when the plaintiff has lost substantial amounts of money resulting from the cyber fraud, which can be recovered through civil proceedings. It is also observed that there is not much the plaintiff can do when the defendant raises *lis pendens* or *res judicata*. This is the gap that the legislature should consider to close in the near future.

The United Kingdom has statutes that regulate cyber fraud in different context. It is also observed that the United Kingdom courts apply the six principles of *res judicata* when there are other matters pending before other courts. The approach followed by the courts in the United Kingdom appears to be more strict. It is suggested that the United Kingdom should consider amending the provisions of section 2 of the Fraud Act so that cyber fraud is expanded on to ensure that perpetrators do not repeat committing cyber fraud in the future. Lastly, it is evident that the application of section 8 of the Cybercrimes Act in Civil Procedure is indeed a hailing snow.

References

Ambrose, H. et al. (2021) *Blackstones's Civil Practice* (21st ed.). Oxford University Press, United Kingdom.

Andrews, N. (2019).*Court Proceedings, Arbitration & Mediation* (2nd ed.). Intersentia, Cambridge.

Broodryk, T. (2019). *Eckard's Principles of Civil Procedure in the Magistrates' Courts* (6th ed.). Juta, Cape Town.

Cassim, F. (2011). Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South African and other regional role players. *The Comparative and International Law Journal of Southern* Africa, Vol.44.No.1, p.123-138. htttp://dx.doi.org/10.17159/1727-3781

Cassim, F. (2009). Formulating Specialised Legislation to Address the growing spectre of Cybercrime: Comparative Study. *Potchefstroom Electronic Law Journal,* Vol.12.No.4, p. 43 ISSN.1727-3781

Pete, S. et al. (2017). Civil Procedure A Practical Guide (3rd ed.). Oxford University Press, South Africa.

Snail, S. (2009). Cybercrime in South Africa – Hacking, Cracking and other unlawful online activities. Journal of Information, Law & Technology, p. 1-13.

Whitty, M.T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, Vol.26.No.1, p. 277-292. https://doi/10.1108/JFC-10-2017-0095

Van der Merwe, D. et al. (2016) *Information and Communications Technology Law* (2nd ed.). (LexisNexis Durban)

Statutes

Communications Act of 2000.

Computer Misuse Act of 1990.

Cybercrime Act 19 of 2020.

Data Protection Act of 2018.

Electronic Communications and Transactions Act 25 of 2002.

Fraud Act of 2006.

Cases

Catalyst Investment Group Ltd c Lewinsohn and Others 2009 EWHC 1964 (Ch).

Ceasorstone Sdot-Yam Ltd v The World of Marble and Granite CC (741/12) 2013 ZASCA 129 (26 September 2013).

Fouries v Van der Spuy and De Jongh Inc. and Others 2020 1 SA 560 (GP).

Hassen v Berrage NO 2012 6 SA 329 (SCA).

Henderson v Henderson (1843-60) All E.R Rep.378.

Ivey v Genting Casinos UK Ltd t/a Crockford 2017 UKSC 67.

Msomi v S 2020 1 SACR 197 (ECG).

R v Ghosh 1982 EWCA Crim 2.

Socratous v Grindstone Investments 2011 6 SA 325 (SCA).

Virgin Altantic Airways Ltd v Zodiac Seats UK Limited 2013 UKSC 46.

WM Morrisson Supermarkets PLC v Various Claimants 2020 UKSC 12.