Received: 15 July 2025, Accepted: 9 August 2025, Published: 9 September 2025, Doi: https://doi.org/10.62726/tlj.v5.79

Delict in Cyberspace in South Africa: Reflection on Recent Judicial Developments

Desmond Oriakhogba* and Nompumelelo Ndwandwe**

Abstract

This article explores the judicial application of the law of delict in cyberspace issues in South Africa. This exploration takes place against the backdrop of the risks of harm, such as pure economic loss, occurring in cyberspace, especially those resulting from the exercise of professional duties. Specifically, the article examines how recent case law, such as Edward Nathan Sonnenberg Inc v Hawarden *[2024] ZASCA 90, addressed the gaps existing in the law of delict on the question of liability for patrimonial harm occasioned by third-party fraudsters in cyberspace. The article further examines the courts' application of the constitutional values of dignity, fairness and freedom to the development and application of the law of delict in addressing harms in cyberspace. As noted in the article, recent case law demonstrates the extent of the legal duties of professionals, their clients and third parties impacted by the exercise of professional duties to prevent patrimonial harm occasioned by the activities of fraudsters in cyberspace in South Africa. The case law marks a significant step towards solving problems caused by emerging cybersecurity challenges, addressing the gap in the law of delict concerning liability for online scams causing pure economic harm.*

Keywords

cyberspace, cyber delict, pure economic harm, professional duty, South Africa

1. Introduction

As digital technology continues to develop, there appears to be an integration of the physical world and cyberspace, which is demonstrated by our unavoidable dependence on digital technology in our daily communication, business activities, as well as the resulting risks and harms that raise challenging questions in the field of the law of delict, as discussed in part 2 below. Indeed, as part of our daily life, cyberspace continues to challenge the remit of the existing legal frameworks, including the law of delict, and the courts are increasingly grappling with the emergence of what has been termed 'cyber delict'[1] in South Africa.

1 Etsebeth, V 'Cyber Delict – Que Sera Sera?' (2008) *Without Prejudice* 42.

* LLB LLM (Uniben) PhD (UCT); Associate Professor, Private Law Department (University of the Western Cape) <https://orcid.org/0000-0003-3078-4320> e-mail: doriakhogba@uwc.ac.za

** Final-year LLB student, Faculty of Law (University of the Western Cape) e-mail: 4157868@myuwc.ac.za

The term 'cyber delict' – or 'cyber tort' as used in other common-law countries[2] – is not used here to indicate any special type or class of delict. The term was coined in a 2008 article written by Verine Etsebeth,[3] and is used here for convenience to describe those activities in cyberspace that may result in delictual wrongs, including defamation and pure economic loss, among other things. Cyber delict is explained further below. It suffices now to note that cyber delict has spurred a discourse on the extent to which the traditional principles of the law of delict can address the surge in delictual actions occurring in cyberspace.[4] Recent case law has reinforced the need to further engage in this discourse in order to determine whether the court's application of delictual principles in this case has closed an important gap relating to pure economic harm resulting from wrongful conduct in cyberspace.[5]

According to Loubser and Midgely,[6] the courts are 'increasingly confronted with cyber-delict', such as online defamation.[7] However, 'it is only a matter of time before courts are confronted with patrimonial harm issues such as […] pure economic harm in the cyberspace'.[8] Also, the risk of pure economic harm associated with cyberspace 'is especially encountered in conveyancing transactions, where fraudsters may attempt to intercept email communications between the attorney and the client and attempt to divert money into fraudulent accounts'.[9] In such situations, 'would the legal convictions of the community dictate that an attorney who does not exercise proper care when interacting online or via email be held liable in delict for damages? What are the policy considerations that would favour or militate against the imposition of liability in such cases?'[10]

Based on a desktop review, we reflect on recent case law, especially the High Court's decision in *Hawarden v Edward Nathan Sonnenberg Inc* ('*ENS* High Court'),[11] and the Supreme Court of Appeal's (SCA) decision in *Edward Nathan Sonnenberg Inc v Hawarden* ('*ENS* SCA'),[12] against the backdrop of the emerging South African jurisprudence relating

2 Holschuh, J '#civilrightscybertorts: Utilizing Torts to Combat Hate Speech in Online Social Media' (2018) 82(3) *University of Cincinnati Law Review* 953; Georgescu, GG, Marin, PM & Vasile, D 'Jurisdiction over Cyber Torts under Brussels I BIS Regulations' (2016) <https://portal.ejtn.eu/PageFiles/14777/Written%20paper_Romania.pdf> accessed 15 July 2025.

3 Etsebeth (note 1).

4 Iyer, D 'An Analytical Look into the Concept of Online Defamation' (2018) 32(2) *Speculum Juris* 125; Marx, FE 'Iniuria in the Cyberspace' (2010) 31(1) *Obiter* 146; Roos, A & Slabbert, M 'Defamation on Facebook: Insparta v Richter 2013 6 SA 529 (GP)' (2014) 17 *Potchefstroom Electronic Law Journal* 2849; Alheit, K 'Delictual Liability Arising from the Use of Defective Software: Comparative Notes on the Positions of Parties in English Law and South African Law' (2006) 39(2) *Comparative and International Law Journal of Southern Africa* 26; Khan, F 'The Impact of COVID-19 on Cyberbullying: A Delictual Claim for Emotional Harm?' (2021) 54 *De Jure* 565.

5 *Edward Nathan Sonnenberg Inc v Hawarden* [2024] ZASCA 90; *Hawarden v Edward Nathan Sonnenberg Inc* [2023] ZAGPJHC 14; *Ndlozi v Media 24 t/a Daily Sun and Others* [2023] ZAGPJHC 1040. See also *RM v RB* 2015 (1) SA 270 (KZP); *Heroldt v Wills* 2013 (2) SA 530 (GSJ).

6 Loubser, M & Midgley, R *The Law of Delict in South Africa* (OUP 2017) 332.

7 Ibid at 16.

8 Ibid.

9 Ibid at 332.

10 Ibid.

11 *Hawarden v Edward Nathan Sonnenberg Inc* (note 5).

12 *Edward Nathan Sonnenberg Inc v Hawarden* (note 5.

to the application of delictual principles to cyberspace. The article begins – in the second part – by examining the development of the law of delict in South Africa to demonstrate the evolution of the principles and rules applicable to the physical world, but adaptable to the present virtual reality made possible by digital technology. The second part also deals with the role played by the Constitution of the Republic of South Africa, 1996 (Constitution) in adapting delictual principles to cyberspace, especially in view of the need to uphold the constitutional values of dignity, fairness and freedom. The third part reviews the *ENS* High Court and SCA cases, while the fourth part discusses the implications of the judgments in the cases. The fifth part concludes the article.

2. Applying the law of delict to cyberspace: A South African perspective

2.1 The interaction between cyberspace and delict

The law of delict is a branch of private law, which plays a crucial role in providing civil remedies for personal injuries, damage to property, and violation of personality rights by wrongful conduct. The fundamental premise in the law of delict is that harm rests where it falls; that is, each person must bear the damage they caused.[13] However, in certain legally recognised situations the burden of damage is transferred from one individual to another, resulting in the latter being obligated to bear the former's damage or provide compensation for it.[14] Neethling and Potgieter accurately identify the conditions under which a person, according to the law of delict, must bear the damage that they have caused to another, thereby incurring civil liability for that damage.[15] For instance, when damage results from a delict, the wrongdoer is legally required to compensate the aggrieved party.

Delictual liability is governed by a generalising approach, which means that general principles relating to the need to prevent harm to persons and property, to promote freedom and fairness, to uphold human dignity, and to maintain societal *boni mores* regulate delictual liability.[16] Thus, to be held delictually liable, there must be a causal (factual and legal) link between the harm suffered by the plaintiff and the wrongful conduct of the person who is at fault.[17] In *H v Fetal Assessment Centre*, the court held that 'harm-causing conduct is a prerequisite for further enquiry into the other elements of delict, namely wrongfulness and fault. Without harm-causing conduct, there is no conduct which can be wrongful or committed with the requisite degree of fault.'[18] These principles apply irrespective of which individual interest is impaired, and regardless of how and where the impairment is caused.[19] Based on this, the law of delict in South Africa can accommodate changing circumstances and new situations more efficiently.[20] Indeed, although South African law of delict developed ages ago in the physical world as demonstrated by its common-law

13 Neethling, J & Potgieter, J *Law of Delict* (LexisNexis 2015) 18.
14 Ibid at 18.
15 Ibid.
16 Loubser & Midgley (note 6) 4-25.
17 *H v Fetal Assessment Centre* [2006] 4 All SA 541 (SCA) para 1.
18 Ibid.
19 Loubser & Midgley (note 6) 5.
20 Alheit (note 4); Khan (note 4).

origins,[21] delictual principles are adaptable and have evolved to the extent that they are applicable to wrongs occurring in cyberspace. Moreover, owing to its flexibility and pliancy, the law of delict has developed to meet societal needs that have emerged in modern times.

The rise of accessible digital technologies and the expansion of the internet have given rise to new forms of behaviour that may result in harm being suffered in cyberspace. Cyberspace is a virtual environment of online communication and data exchange.[22] Unfortunately, it is also a realm where wrongful acts can cause harm to others. Klein AJ judicially acknowledged this much in *Fourie v Van Der Spuy and De Jongh Inc. and Others*,[23] where the judge noted that the 'rate at which cybercrime occurs makes the internet a very unsafe working area'.[24] Cyber criminals and hackers exploit the internet for monetary gain, while others perceive cyberspace as a platform for unbridled information exchange and expression of opinions.[25] De Vos aptly captures this phenomenon by noting that 'there is something about internet websites and social media platforms that seem to bring out the worst in people. Reasonably decent people who might well carefully weigh their words can become raving hatemongers and irresponsible tattletales on these platforms.'[26]

Specifically, the practice and business of law in South Africa is not insulated from the risks of harm occurring in cyberspace as a result of the activities of cyber fraudsters. Recognising such risks, key standard-setting bodies in the legal profession in South Africa continue to issue advisories on how to ensure safety in cyberspace while conducting the business of the law.[27] For instance, in 2018, the Law Society of South Africa (LSSA) issued a cybercrime advisory, calling on attorneys to be aware of the dangers of business email compromise (BEC), especially in relation to their clients.[28] The advisory was 'aimed primarily at attorneys fulfilling their duty of care to clients by making them aware of the potential risk' of BEC.[29] It urged attorneys to warn clients of the risk and recommended a model warning that should be contained in communications between attorneys and their clients.[30]

Notably, aside from the difference in the modus and medium of occurrence, harm suffered in cyberspace as a result of cybercrime does not differ from harm in the physical world. Examples of delict in cyberspace include online defamation, where false and defamatory comments made through digital platforms or emails harm someone's reputation.[31]

---

21 Loubser & Midgley (note 6) 16.
22 Mabeka, NQ & Cassim, F 'Interpreting the Provisions of the Cybercrimes Act 19 of 2020 in the Context of Civil Procedure: A Future Journey' (2023) 44(1) *Obiter* 19.
23 *Fourie v Van Der Spuy and De Jongh Inc. and Others* [2019] ZAGPPHC 449.
24 Ibid para 25.
25 Mabeka & Cassim (note 22).
26 Cited in Iyer (note 4) 125.
27 Legal Practice Council Fraud Alert (2020) <https://www.derebus.org.za/wp-content/uploads/2020/07/Notice_Fraud-alert-to-Legal-Practitioners.pdf> accessed 15 July 2025; LSSA 'LSSA Advisory: Cybercrime: Business Email Compromise' (2018) <https://www.lssa.org.za/news/lssa-advisory-cybercrime-business-email-compromises/> accessed 15 July 2025. The Legal Practitioners Indemnity Insurance Funds frequently publishes cybercrime risks alerts. <https://lpiif.co.za/2023/?post_type=aiif_risk> accessed 15 July 2024.
28 LSSA ibid.
29 Ibid.
30 Ibid.
31 See *Ndlozi* (note 5).

Hate speech, expressed through derogatory posts based on race, gender or sex, for example, is another form of harm in cyberspace (which may also be criminal), especially where it violates personality rights such as personal integrity and dignity.[32] BEC, a form of cyber fraud where fraudsters trick an unsuspecting recipient of business emails into divulging company secrets or paying money to them, is a further example of conduct resulting in harm occurring in cyberspace.[33] BEC may give rise to pure economic loss, as occurred in the *ENS* High Court and SCA cases (discussed below).

Understanding the effect of cyberspace as both a medium of expression and a source of harm is crucial within the framework of the Constitution. The digital realm has become a dominant platform for communication, allowing individuals to express their thoughts, share information, and connect with others across the globe. This vast reach and accessibility underscore the importance of protecting freedom of speech and expression, as enshrined in constitutional principles. However, cyberspace also presents significant challenges, particularly concerning the potential for harm. Online defamation, for instance, illustrates how false and defamatory statements can rapidly spread across digital platforms, causing substantial damage to an individual's reputation. The anonymity and speed of the internet can exacerbate these issues, making it difficult to trace the source of harmful content and to mitigate its impact effectively.

Therefore, within the constitutional framework, a delicate balance must be maintained between safeguarding free expression and protecting individuals from harm. Legal provisions must address the unique nature of cyberspace, ensuring that while the right to free speech is upheld, mechanisms are in place to hold individuals accountable for wrongful actions, such as defamation. This balance is essential for fostering a safe and just digital environment where the rights of all users are respected and protected.

2.2 The role of the Constitution in shaping delictual principles online

According to the Constitutional Court in *Carmichele v Minister of Safety and Security*:[34]

> [The] common law, especially in the field of delictual liability, has constantly required development. Where a court develops the common law, the provisions of section 39(2) of the Constitution oblige it to have regard to the spirit, purport and objects of the Bill of Rights. … This requires not only a proper appreciation of the Constitution and its objective, normative value system, but also a proper understanding of the common law. … Not only must the common law be developed in a way which meets the section 39(2) objectives, but it must be done

32 Burchell, J 'Balancing "Equality of Respect" with Freedom of Expression: The Actio Iniuriarum and Hate Speech' in Bradfield, G, Fagan, A & Scott, H (eds) *Private Law in a Changing World: Essays for Danie Visser* (Juta, 2020) 203-227; Len, LKLTS & De Ruijter, A 'Conceptualising the Tortuous Harms of Sexist and Racist Hate Speech' (2023) 2(1) *European Law Open* 8; Holschuh (note 2).

33 Orekeng, KS 'The Dangers of Business E-mail Compromise' (2023) *De Rebus* <https://www.derebus.org.za/the-dangers-of-business-e-mail-compromise/> accessed 15 July 2025; LSSA (note 25); SABRIC 'Business Email Compromise' <https://www.sabric.co.za/stay-safe/business-email-compromise/> accessed 15 July 2024.

34 *Carmichele v Minister of Safety and Security* [2001] ZACC 22.

> in a way most appropriate for the development of the common law within its own paradigm.[35]

Although the above case does not relate to delict in cyberspace,[36] the Constitutional Court's guidance is important when examining claims based on harm suffered online, especially where they raise questions relating to advancing the law of delict through a constitutional lens. Thus, the advancement of delictual principles and rules to accommodate harm suffered in cyberspace in South Africa must be pursued through the prism of the Constitution, especially given the requirement that the development of the law of delict, like other common law, must align with and uphold the constitutional values of human dignity, equality and freedom embedded in the Constitution.[37]

The foregoing represents the judicial attitude demonstrated in *Heroldt v Wills*,[38] where the High Court addressed the issue of defamation on social media. In that case, an interdict was granted against the defendant for posting derogatory messages about the plaintiff, suggesting that he was an unfit father to his girls because of 'the alcohol, the drugs, the church'.[39] The defendant had initially declined to remove the posts, arguing that she had the right to freedom of expression, which the court had to balance against the plaintiff's right to privacy and dignity.[40] The court emphasised the importance of balancing the right to freedom of expression with the right to dignity, protected under the Constitution.[41] The court acknowledged the transformative impact of digitisation on communication and the potential for harm in cyberspace.[42] Thus, it clarified that defamatory statements made on social media platforms have the potential to cause significant damage to a person's reputation.[43] Moreover, the court considered the constitutional values of dignity and freedom of expression, striking a balance to protect individuals from harm while respecting the right to express opinions.[44] Importantly, this case underscores the dynamic nature of delictual principles in the face of technological evolution and the imperative for the common law to be adapted in line with constitutional values.

In *RM v RB*,[45] Chetty J delineated the boundary for our courts concerning the protection of social media users. The case involved a family. Citing concerns about the father's use of alcohol and drugs, the mother took to Facebook to criticise the father's care of their daughter, who had previously spent the weekend with him. Chetty J noted that while courts have the authority to compel the removal of defamatory messages from social media, they should refrain from issuing orders that prevent individuals from expressing

35 Ibid paras 35 and 55.
36 For a discussion of the case, see Fagan, A 'Reconsidering *Carmichele*' (2008) 125(4) *South African Law Journal* 659.
37 Section 1(a) of the Constitution of the Republic of South Africa 1996.
38 *Heroldt* (note 5).
39 Ibid para 7.
40 Ibid.
41 Ibid para 6.
42 Ibid para 8.
43 Ibid para 6.
44 Ibid para 7.
45 *RM v RB* (note 5).

themselves through social media or other means.[46] This reasoning effectively strikes a balance between the constitutionally enshrined right to freedom of expression and the right to dignity.[47] The court proactively advanced the development of the law of delict by incorporating constitutional values into its framework. By doing so, the court underscored the importance of upholding individual rights while also acknowledging the complexities of modern digital interactions. Consequently, the court's jurisprudential evolution reflects a dual commitment to constitutional principles and an acute awareness of the challenges and potential harms in cyberspace. This approach ensures that the law remains relevant and responsive to contemporary issues, providing robust protection for individuals without undermining their fundamental freedoms.

In *Le Roux v Dey*,[48] a compelling precedent in South African legal history was set, addressing harm that results from student activities in cyberspace. In this instance, the first defendant crafted a computer-generated image at his residence, superimposing the likenesses of his school's principal and deputy principal onto a picture featuring two unclothed male bodybuilders in a sexually suggestive pose.[49] The school's emblems were overlaid onto the genital areas of the individuals in the image.[50] The first defendant then shared this manipulated image with a fellow student via computer. The second and third defendants further propagated the image by distributing it among numerous other students at the high school.[51] The principal and deputy principal were in an embarrassing situation. Despite disciplinary measures having been taken against the students involved, unfounded rumours persisted at the school, which continued to harm the dignity of the deputy principal. In response, the deputy principal took legal action, seeking damages for defamation and arguing that his right to human dignity had been infringed. The case eventually reached the Constitutional Court, where the students defended their actions by arguing that the image was merely a schoolboy prank and lacked any defamatory intent.[52] The Constitutional Court, however, rejected the defendants' claim of lacking intention, recognising the fundamental importance of respecting school authority figures for maintaining discipline – a crucial element for the proper functioning of the education system. The court acknowledged a growing trend in South African schools to challenge the status and authority of teachers, leading to a breakdown in discipline.[53] Consequently, the court affirmed the defamatory nature of the manipulated computer image and mandated that the students apologise and pay compensation to the plaintiff.[54] This decision highlights that defamatory actions, especially those that affect the dignity of educators or students, whether they occur within or outside the school environment and involve cyber-related

46 Ibid para 276.
47 Ibid.
48 *Le Roux v Dey* [2011] ZACC 4.
49 Ibid para 13.
50 Ibid para 14.
51 Ibid.
52 Ibid.
53 Ibid para 24.
54 Ibid.

activities, not only breach South African common law but also violate constitutional principles by undermining an individual's dignity.

In *Roestoff v Cliffe Dekker Hofmeyr Inc*,[55] the plaintiff, an attorney, brought a legal action against the defendant, a firm of attorneys. The plaintiff maintained a private bank account with Absa, while the defendant managed trust accounts with Standard Bank and Nedbank. The plaintiff sought to recover funds from the defendant, as money from his personal account had been routed by an internet fraudster through the law firm's trust account. The law firm, unaware of any wrongdoing, treated the transaction as genuine and disbursed the funds to a closed corporation, acting on instructions purportedly from a client who had supplied the necessary documents. Everything appeared in order at the time, and the firm, in good faith, executed the transfer. Du Plessis J determined that the law firm exhibited no negligence in its actions since it did not know that the funds originated from a scam. The court, per Du Plessis J, emphasised that once an owner's funds are deposited and mingled with other funds in an account, the original owner loses control over it. The court further underscored that the law firm was oblivious to the fact that the money belonged to the plaintiff and originated from a scam. The court noted that the plaintiff did not dispute seeing warnings about phishing scams but claimed not to have read them' the court deemed this to be neglectful.[56] The court, therefore, concluded that the defendant acted in good faith and without negligence, and was not liable for the restitution of the funds. The court absolved the defendant of any obligation to repay the plaintiff. In the context of this article, the significance of the case rests on the court's recognition of the general duty of attorneys in respect of moneys deposited in their trust accounts. The court ruled that attorneys have a legal duty to depositors of money in their trust accounts. Attorneys also owe this legal duty to persons who are not their clients.[57] According to the court, an attorney's:

> legal duty is broad enough to include that the defendant in this case, even though he did not know who the plaintiff was, had a legal duty to the plaintiff to, without negligence, deal with the deposit in the trust account. In my view, the key question in this case is whether the defendant was negligent. I therefore accept without finding that the defendant had a legal duty to the plaintiff to deal with the deposit in a way that would not cause harm to the plaintiff.[58]

Finally, in *Ndlozi v Media 24*,[59] the High Court, per Wilson J, ruled that online reports by the defendant were unlawful and defamatory.[60] The court ordered the defendant to promptly remove reports, which falsely accused the plaintiff of rape, from all its media platforms, including its website, Twitter account and Facebook account.[61] The court's application of

55 *Roestoff v Cliffe Dekker Hofmeyr Inc* 2013 (1) SA 12 (GNP).
56 Ibid para 81.
57 Ibid paras 71, 82 and 83.
58 Ibid para 83.
59 *Ndlozi* (note 5).
60 Ibid.
61 Ibid para 72.

delictual principles and its rejection of any public interest claim was crucial in a case of delict because it ensured the proper adherence to the legal framework governing wrongful acts, emphasising the protection of individual rights against defamation. The rejection of any claim of public interest in publishing defamatory content highlights the need to balance freedom of expression with the rights of individuals. While freedom of speech is a fundamental right, it is not absolute and must be exercised responsibly, especially with regard to potentially harmful speech. By refusing to prioritise public interest over the protection of individual rights, the court reinforced the principle that rights and freedoms are not to be arbitrarily infringed upon, even in the name of public discourse. The court underscored that the harm caused by disclosing a rape complaint at an early investigative stage outweighed any potential public benefit.[62] The court held that the reports were defamatory and unlawful, emphasising that the defendant's actions interfered with a police investigation by prematurely publishing the complaint.[63] Underscoring the important role that constitutional values play in cases of this kind, the court noted that:

> [T]he inquiry into whether a publication is for the public benefit is also generally the stage of deliberation at which a court will balance the right to freedom of expression, including media freedom, against the right to dignity of the person defamed … . In my view, that balancing act must take place against the backdrop of 'the appropriate norms of the objective value system embodied in the Constitution' … . That value system embraces, I think, a confidentiality interest that does not just protect the suspect's right to dignity. It also protects the integrity of the police investigation. Most importantly, in a case like this, it protects the dignity and privacy of the complainant. … [T]he right to privacy 'seeks to foster the possibility of human beings choosing how to live their lives within the overall framework of a broader community. The protection of this autonomy, which flows from our recognition of individual human worth, presupposes personal space within which to live this life.' … [T]hat autonomy encompassed the right to choose whether, when and how to disclose intimate details about one's private life.[64]

This case demonstrates the instrumental role played by the Constitution in the evolution and application of delictual principles to cyberspace in South Africa. Importantly, the case further underscores the adaptability of the law of delict in adjudicating not only physical realm cases but also those arising in cyberspace.

3. The *ENS* High Court and SCA cases

The brief facts in the *ENS* High Court case were that the plaintiff purchased immovable property from a seller who appointed the defendant as the conveyancer to handle the sale. Under the sale agreement, the plaintiff paid a deposit for the purchase price and agreed to pay the balance of R5.5m through an electronic funds transfer (EFT) to the defendant's trust

62 Ibid para 70.
63 Ibid para 69.
64 Ibid paras 63-64.

account for the seller's benefit pending the registration of the transfer. The defendant's account details were sent to the plaintiff via email. Through BEC, the payment made by the plaintiff was intercepted and diverted by an internet fraudster. The plaintiff suffered patrimonial loss as a result and instituted an action against the defendant for the loss of 5.5 million sustained by her as a result of the cyber fraud. The plaintiff succeeded in the High Court, but failed in the SCA. This part sets out the issues considered and decisions reached by the High Court and the SCA. The next part comments on the positions of the courts.

3.1 Issues raised in the High Court

The legal question in the High Court was whether the defendant, a conveyancing firm, was negligent in the manner in which they sent their account details to the plaintiff and should be held liable for the patrimonial harm incurred through BEC. The plaintiff and a secretary in the conveyancing department of the defendant had been emailing back and forth about the property that the plaintiff was purchasing. The defendant represented the latter.[65] Cyber-criminals compromised the plaintiff's email inbox, and she paid the amount she owed on the property into the wrong bank account.[66] Subsequently, she claimed that the defendant, as a qualified attorney with enormous conveyancing experience, ought to have known of the risks of BEC and should have taken steps to prevent it from occurring. The plaintiff claimed that the defendant owed her a duty of care and its failure to exercise that duty gave rise to the BEC that led to the pure economic loss that she suffered. Accordingly, the plaintiff claimed that the defendant was liable to her for the pure economic loss that she had suffered.[67]

The defendant's argument was based on the premise that, should the court find it liable, this would set a precedent that would expose all conveyancing firms, regardless of size, to similar claims from third parties with whom they have no direct relationship.[68] These claims would stem from losses incurred due to fraudulent activities, such as the hacking of email accounts.[69] The defendant emphasised that such a ruling would impact not only law firms but also all businesses that commonly transmit invoices, including their banking details, via email – a widespread practice, according to the defendant.[70] Moreover, the defendant argued that the prevailing norm in the marketplaces is that the responsibility lies with the debtor, particularly when opting for electronic payments, to ensure that funds are directed to the correct account.[71] In light of this, the defendant urged the court to resist expanding liability for pure economic loss in this instance, citing the Constitutional Court's caution, in *Country Cloud Trading CC v MEC, Department of Infrastructure Development*,[72] against creating 'liability in an indeterminate amount for an indeterminate time to an indeterminate class'.[73]

65 *ENS* High Court (note 5) para 6.
66 Ibid para 15.
67 Ibid.
68 Ibid para 112.
69 Ibid.
70 Ibid.
71 Ibid para 113.
72 *Country Cloud Trading CC v MEC, Department of Infrastructure Development* 2015 (1) SA 1 (CC).
73 *ENS* High Court (note 5) para 113.

3.2 Decision of the High Court

The court held that the defendant has a legal duty to 'prevent harm resulting from the conveyancer's failure to warn the depositor of the dangers of cyber hacking and spoofing of emails or of the fact that PDF attachments to emails containing sensitive information such as bank account details are not invulnerable to BEC'.[74] The court held further that 'the interests of the defendant as well as the society demand that a legal duty is recognised in this case'.[75] The court followed the *dictum* in *Estate Van der Byl v Swanepoel*,[76] and held that 'where one of two innocent parties have to suffer a loss arising from the misconduct of a third party it is for the public advantage that the loss should fall … on that one of the two who could most easily have prevented the happening or the recurrence of the mischief'.[77] Thus, the court held that ENS is a sophisticated commercial entity and is well-positioned to foresee the risk of BEC occurring. Individuals in society need to be better placed to respond to the ever-evolving threat of cybercrime, which is sophisticated and technical.[78] Moreover, the defendant, an experienced conveyancer, was aware of the inherent risks in conveyancing transactions based on its prior knowledge of the dangers of BEC.[79] The foreseeability of the risk of BEC imposed a duty on the defendant to take precautions against potential harm, and its failure to do so was deemed negligent in the given circumstances.[80]

Furthermore, the court held that 'the facts that are common cause and as found regarding this matter leave no doubt …, but for the negligent transmission of its account details and failure to warn [the plaintiff] upfront of the inherent danger of BEC, she would not have suffered the loss'.[81] The court stated that the defendant was the factual cause of the plaintiff's loss, as it provided its bank account details and was responsible for their accuracy and secure transmission.[82] On the enquiry relating to legal causation, the court held that the negligent conduct of the defendant was linked sufficiently closely or directly to the loss suffered by the plaintiff, given that the loss was reasonably foreseeable under the circumstances.[83] Consequently, the court concluded that it was reasonably foreseeable under the circumstances that the plaintiff might suffer loss as she did. Thus, ENS was the proximate cause of the plaintiff's harm. Legal causation was also established, as the defendant's negligent conduct was sufficiently linked to the plaintiff's loss, given that the loss was reasonably foreseeable under the circumstances.[84]

Additionally, the defendant's failure to ensure the safe transmission of the account details was considered wrongful conduct. In assessing wrongfulness, the court determined

74 Ibid para 126.
75 Ibid para 131.
76 *Estate Van der Byl v Swanepoel* 1927 AD 141.
77 Ibid at 150.
78 *ENS* High Court (note 5) para 117.
79 Ibid para 131.
80 Ibid para 130.
81 Ibid para 129.
82 Ibid.
83 Ibid.
84 Ibid para 129.

that the plaintiff's loss, in this case, was quantifiable and determinate, mitigating concerns about indeterminate liability as a policy consideration against recognising liability for pure economic loss.[85] The court also found that factual causation was established because, but for the defendant's negligent transmission of its bank account details and failure to inform the plaintiff of the risks of BEC, the plaintiff would not have suffered the loss.[86] As a result, the High Court ordered that the plaintiff's claim be upheld, with costs on the scale typically applicable between an attorney and its client, including the costs incurred for the engagement of two counsel.

3.3 Issues raised at the SCA

The defendant, ENS (as appellant), appealed against the decision of the High Court.[87] The issue before the SCA was whether the plaintiff (as respondent) had adequately established the element of wrongfulness for a delictual claim arising out of an omission causing pure economic loss. At the SCA, the parties offered the same arguments that they had advanced before the High Court, which are discussed above.

3.4 Decision of the SCA

The SCA's decision was based on the principle that individuals are generally not liable in delict for losses caused by omission, unless there is a legal duty to act.[88] In this instance, the SCA found that no such legal duty existed between ENS (the appellant) and Ms Hawarden (the respondent).[89] This was because there was no contractual relationship between ENS and Ms Hawarden and, thus, her loss occurred at a time when there was no attorney–client relationship.[90] Pursuant to this, the SCA held that the respondent suffered loss, not as a result of any failure in the appellant's system, but because hackers had infiltrated her email account and fraudulently diverted her payment meant for the appellant into their own account.[91] The interference that caused the loss was a result of the respondent's email account having been compromised.[92]

From the records, the SCA found that the respondent had earlier been warned via letter of the risk of BEC. Consequently, the SCA held that it would have been fairly easy for the respondent to have avoided the risk.[93] As the respondent did with the estate agent, she should have verified the appellant's bank account details before making the payment.[94] The court held that the respondent had ample means to protect herself from the loss in view of the fact that there was an active line of communication between her and the appellant before the payment was made, as well as the option of a bank guarantee for cash transfer,

85 Ibid para 130.
86 Ibid.
87 *ENS* SCA (note 5).
88 Ibid para 19.
89 Ibid.
90 Ibid para 20.
91 Ibid.
92 Ibid.
93 Ibid.
94 Ibid.

which she failed to take advantage of.[95] Furthermore, the SCA clarified that any warning by the appellant of the risk of BEC would have been meaningless, in the circumstances of this case, because by that time the cybercriminal was already embedded in the respondent's email account, and consequently the risk had already materialised.[96]

Therefore, the court held that a finding that the defendant's failure to warn the respondent attracted liability would have profound implications not only for the attorneys' profession, but for all creditors who send their bank details by email to their debtors.[97] According to the SCA, the *ratio* of the High Court judgment that all creditors in the position of the appellant owe a legal duty to their debtors to protect them from the possibility of their accounts being hacked is untenable.[98] The SCA concluded that the High Court should have declined to extend liability in this case because of the real danger of indeterminate liability.[99] The appeal was therefore upheld.[100]

4. Reflections on the High Court and SCA decisions

To a large extent, we prefer the High Court's judgment rather than the SCA's judgment. We must, however, note that the strength of the SCA's decision rests on the court's finding that the respondent (Hawarden) had ample opportunities to verify the account details before depositing the money in the account, but failed to take advantage of these opportunities. Moreover, there was evidence that the estate agent had initially warned the respondent about the risks of BEC. Even so, we believe that the appellant's omission does not completely absolve the appellant, as a firm of attorneys and professional conveyancers, of liability for its failure to discharge their professional duty towards the respondent. Indeed, the respondent was not the direct client of the appellant. However, as demonstrated below, the case law shows that a professional's legal duty to act with care, skill, and diligence extends to third parties in whose favour it acts, pursuant to the direct contractual relationship between it and its clients.[101] We turn to this later. For now, we should note, however, that the respondent's failure to use the alternative opportunities to confirm the account details should have been regarded as contributory negligence, with the effect of being apportioned a share of the damages at best. Unfortunately, this issue was not raised in the SCA.

The evolution of cyberspace has ushered in a paradigm shift in legal considerations, challenging traditional delictual principles and requiring a careful examination of their applicability in this new realm. The *ENS* SCA and High Court cases provided a pivotal moment where the judiciary confronted the complexities of pure economic harm caused by BEC, a relatively recent addition to the jurisprudence on delict in cyberspace in South Africa. Notably, the High Court applied the well-established elements of harm, conduct, causation, fault and wrongfulness, akin to those used in adjudicating delict actions in the physical world, demonstrating the adaptability of the law to address emerging challenges.

95 Ibid para 26.
96 Ibid para 20.
97 Ibid para 21.
98 Ibid.
99 Ibid.
100 Ibid.
101 *Roestoff* (note 55).

The established precedent of the court in *casu*, particularly in evaluating wrongfulness, has significantly influenced and demonstrated the adaptability of the law of delict to the advancements in technology. As a key determinant of liability, wrongfulness involves evaluating whether it is reasonable to impose legal responsibility on the defendant for the harm resulting from their conduct.[102] In *Gerber v PSG Wealth Financial Planner*,[103] the court held that PSG had to compensate Gerber for financial losses incurred due to cybercriminal activities. This decision was grounded in PSG's contractual obligations and failure to implement adequate security measures, providing a clear basis for liability.[104]

Similarly, the *ENS* case involved a compromise of the respondent's email systems, leading to cybercriminals impersonating the appellant's email address. Unlike the PSG scenario, however, the respondent and the appellant in the *ENS* SCA and High Court cases had no direct contractual relationship. Even so, as held in *Roestoff v Cliffe Dekker Hofmeyer*,[105] the legal duty owed by attorneys in relation to money deposited in their trust account is broad enough to cover both their clients and third parties who are not their clients.[106] Moreover, an established principle of the South African law of delict is that the negligent performance of a contractual duty, especially by a professional, that results in pure economic loss to a third party can entitle that third party to claim against the professional. It is immaterial that the third party is not a party to the contract.[107] Thus, in examining the intersection of professional liability, contractual obligations and the duty of care of attorneys, it is imperative to recognise the unique characteristics that define the attorney–client relationship. As members of an established and organised profession, attorneys operate within a framework that demands specialised knowledge, skill and care.[108]

As demonstrated in the second part above, the legal profession emphasises the competence of its practitioners, requiring them to adhere to a standard commensurate with the expertise expected from a reasonable person in their profession, especially concerning their dealings in cyberspace. The client–attorney relationship, a quintessential element of legal practice, is inherently contractual. This contractual dimension imposes an implicit obligation on attorneys to perform their professional services with the knowledge, competence and skill reasonably expected of a member of the legal profession. The contractual duty establishes a foundation for the professional conduct of attorneys, ensuring that their clients – including persons for whose benefit their clients have retained their services – receive a standard of service that aligns with the specialised nature of legal practice. Moreover, in the legal landscape, courts have consistently recognised that attorneys may be held liable for delicts concerning pure economic loss suffered by

102 Neethling & Potgieter (note 13) 45.
103 *Gerber v PSG Wealth Financial Planner* [2023] ZAGPJHC 270.
104 Ibid para 52.
105 *Roestoff* (note 55).
106 Ibid paras 81, 82 and 83.
107 For instance, see *EG Electric v Franklin* 1979 (2) SA 702 (E); *Perlman v Zoutendyk* 1934 CPD 151; *Longueira v Securitas of SA* 1998 (4) SA 258 (W).
108 Loubser & Midgley (note 6) 326.

their clients as a result of the attorney's wrongful conduct.[109] This acknowledgement underscores the broader responsibility that attorneys bear beyond the contractual realm as demonstrated in the *ENS* High Court case.

Based on the foregoing, we argue that the SCA erred by narrowly construing the absence of a direct contractual relationship as a ground for absolving the appellant of liability. This approach reflects a regressive and overly simplistic view that fails to align with the dynamic legal landscape required to address the complexities of cyberspace. The SCA's focus on the absence of a direct contract overlooks the broader duties that professionals, particularly attorneys, owe in an interconnected digital world. Legal precedents, such as *Gerber v PSG Wealth Financial Planner* and *Roestoff v Cliffe Dekker Hofmeyer*, emphasise that the duty of care extends beyond the confines of a contractual relationship, especially when dealing with professionals who operate within a framework demanding specialised knowledge, skill and care. The High Court's decision was not only about adhering to precedent, but also about recognising that the legal profession must respond to the challenges posed by cyber threats, which can cause significant economic harm to clients and third parties alike.

Moreover, the High Court rightly identified that the essence of wrongfulness in delict lies in determining whether it is reasonable to impose legal responsibility on the defendant. The firm's failure to warn about potential cyber risks, despite knowing about the increasing prevalence of email fraud, constitutes a breach of the duty of care expected of a legal professional. The SCA's reluctance to impose this duty, under the guise of avoiding 'indeterminate liability', appears to run against the current cyber reality: it fails to appreciate that, in this digital age, the scope of professional responsibility must necessarily expand to address the real and substantial risks posed by cybercrime. It also ignores the fact that delictual liability is determined on a case-by-case basis. Thus, success in one situation is not a guarantee of success in subsequent cases. Moreover, upholding the appellant's liability in the *ENS* SCA case would have aligned the South African law of delict with the principle of negligent enablement of cybercrime emerging in US tort law.[110] By clinging to outdated notions of legal duty and failing to recognise the adaptability of delictual principles in cyberspace, the SCA's decision is a missed opportunity to advance the law in a way that meets the demands of modern technology. The High Court's judgment, which embraces this necessary evolution, provides a more compelling and forward-thinking framework for addressing the challenges of cyber fraud, ensuring that victims are not left without recourse in an increasingly digital world.

Indeed, in *Fourie v Van Der Spuy and De Jongh Inc. and Others*,[111] the High Court confirmed the duty of attorneys in a situation involving loss suffered by a client as a result of the activities of fraudsters in the digital space. The case involved the erroneous payment by the respondents (the attorneys) of the sum of R1 744 599.45 meant for the applicant (their client) to a cyber fraudster, as a result of hacked emails. Holding the respondents

109 Ibid.

110 For a discussion, see Rustad, ML & Koenig, TH 'The Tort of Negligent Enablement of Cybercrime' (2005) 20 *Berkeley Technology Law Journal* 1553.

111 *Fourie* (note 23).

jointly and severally liable to pay the applicant the amount in dispute, the court, per Klein AJ, held that:

> [t]he 2nd Respondent was negligent and failed to exercise the requisite skill, knowledge and diligence expected of an average practising attorney and thus failed to discharge her fiduciary duty to the Applicant by transacting via e-mail whilst fully knowing that fraud is prevalent in her profession and not employing any measures to ensure that neither she nor the Applicant will fall victim to fraud.[112]

Although the above case focused on contractual relations between attorneys and their clients, it is nonetheless relevant in appreciating the importance of the attorney's professional duty in relation to guarding against the risks of BEC. Earlier, the High Court had similarly held an attorney responsible for the loss suffered by its client, as a result of BEC. This was the case of *Jurgens and Another v Volschenk*,[113] where the attorney represented the client in a conveyancing transaction. However, through BEC, the payment from the sale of the property was intercepted by internet fraudsters. According to the High Court, per Tokota J, it is 'the duty of an individual attorney to ensure, as far as she/he is able to do so, that he/she measures up to the high standards demanded of him/her'.[114]

Nonetheless, a crucial nuance emerges in the *ENS* SCA case, where the appellant did not represent the respondent, but was acting on behalf of the property seller. Despite this, the appellant in the *ENS* SCA case remained bound by a legal duty to the respondent, according to *Roestof v Cliffe Dekker Hofmeyer*, as already discussed above. As the High Court correctly noted in the *ENS* case, the appellant (as defendant) was obligated to 'prevent harm resulting from the conveyancer's failure to warn the depositor of the dangers of cyber hacking and spoofing of emails or of the fact that PDF attachments to emails containing sensitive information such as bank account details are not invulnerable to BEC'.[115] Consequently, the appellant demonstrated negligence by failing to alert the respondent to the risks of cyber hacking, an oversight that the High Court correctly highlighted. The appellant, who was in a position to foresee this harm, was held accountable for failing to provide the necessary warnings – a foresight not necessarily apparent to a layperson.

5. Conclusion

To some extent, the SCA erred in its judgment by failing to account for the evolving nature of delictual liability in the context of cyberspace, particularly when addressing the responsibilities of professionals like attorneys in the digital age. The High Court, on the other hand, correctly recognised the need for the law to adapt to the realities of the digital era, where new forms of harm, such as BEC, demand a reassessment of established legal principles. The development of the digital space has introduced unprecedented opportunities and challenges, making it essential for the law to evolve in tandem. The *ENS* SCA and High Court cases mark a pivotal moment in the application of delictual

112 Ibid paras 18, 20, 24 and 30.
113 *Jurgens and Another v Volschenk* [2019] ZAECPEHC 41.
114 Ibid paras 22 and 26.
115 *ENS* High Court (note 5) para 130.

principles to the digital realm, particularly in addressing the liability of attorneys for pure economic loss caused by cyber fraud. The High Court's judgment successfully closes a gap in the law of delict that had previously left victims of BEC and similar online scams without adequate legal recourse.

We have identified the complexities of applying traditional delictual principles to the emerging landscape of cyberspace, emphasising the need for a cautious yet adaptable approach. The High Court's decision reflects this careful balancing act, ensuring that the law protects individuals from the unique risks posed by digital transactions while maintaining the integrity of established legal principles. The SCA's refusal to impose liability on ENS, based on the absence of a direct contractual relationship, fails to recognise the broader duty of care that professionals owe in the digital age. By embracing the adaptability of the law of delict to address the challenges of cyberspace, the High Court demonstrated a forward-thinking approach that protects the values of dignity, fairness and freedom in an increasingly digital world. The SCA's decision, by contrast, represents a step backward, neglecting the judiciary's role in ensuring that legal frameworks evolve to meet the demands of new technologies without compromising fairness or coherence. The High Court rightly struck the balance between tradition and evolution, ensuring that the law remains resilient and capable of addressing the complexities of modern delictual actions in cyberspace.

How to cite:

Desmond Oriakhogba and Nompumelelo Ndwandwe 'Delict in Cyberspace in South Africa: Reflection on Recent Judicial Developments' (2025) 5 *Turf Law Journal* 1-17.