

‘IS SOUTH AFRICA LOAST AT SEA IN THE CRIMINALISATION OF "CATFISHING"? A COMPARATIVE ANALYSIS’

by

Emshareed Botes

Supervisor: Bernice Welgemoed

Submitted in partial fulfilment of the requirements for the degree of
Master of Laws by Coursework and Research Report
at the University of the Witwatersrand, Johannesburg

Date: 29 February 2024

DECLARATION

I, ___1619236_____ declare that this Research Report is my own unaided work. It is submitted in partial fulfillment of the requirements for the degree of Master of Laws (by Coursework and Research Report) at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

I have submitted my final Research Report through TurnItIn and have attached the report to my submission.

Word Count: __10, 171_____ [Incl. the body of your report, footnotes **BUT** excl. title page, declaration, abstract, table of contents and bibliography]

Date: 28 February 2024

ABSTRACT

The infamous form of online impersonation, colloquially known as "catfishing," has become rife globally. Through the boom of technology, especially that of the internet that gave rise to social media- gaining access to other individuals, photographs, personal details, and virtual lives is as easy as pushing a button. Catfishing occurs when individual X utilises the photographs and/or identity of Y. X either pretends to be Y, or X acts as themselves online and utilises the photos of Y to falsify X's true identity when X speaks to Z. Catfishing" generally comprises of impersonation. Still, it does not always comprise of fraud. Several states in the USA, namely; Oklahoma, California, Texas, and New York have criminalised online impersonation as an independent criminal offence from "fraud." Although South African law has delictual remedies and criminalises fraud, it lacks a criminal offence in relation to the impersonation of an individual online, as has been codified in the USA. This essay focuses on the criminalisation of online impersonation (also known as "catfishing") in South Africa through a comparative analysis with the USA, to the exclusion of delictual remedies available in South Africa. This analysis proposes to amend the Cybercrimes Act, with the inclusion of a new section to the Act that focuses specifically on the criminalisation of catfishing through the use of a "scaffolding approach" to categorise the different crimes intrinsic to catfishing.

TABLE OF CONTENTS

DECLARATION.....	Error! Bookmark not defined.
ABSTRACT.....	3
I INTRODUCTION.....	5
II WHAT IS CATFISHING?.....	8
III THE SOUTH AFRICAN POSITION ON CATFISHING.....	11
(a) <i>The law of Delict</i>	11
(b) <i>Common law Fraud</i>	13
(c) <i>The Cybercrimes Act</i>	13
(d) <i>Crimen iniuria</i>	18
IV CATFISHING IN THE USA.....	21
(a) <i>New York</i>	22
(b) <i>California</i>	23
(c) <i>Oklahoma</i>	24
(e) <i>Arizona</i>	26
V ANALYSIS AND RECOMMENDATIONS.....	27
VI CONCLUSION.....	29
VII BIBLIOGRAPHY.....	31

I INTRODUCTION

As of April 2023, it is estimated that there are approximately 5.18 billion Internet users worldwide, and 4.8 billion of the total Internet users worldwide utilise social media.¹ Social media is an umbrella term that refers to social networking sites and platforms that users utilise in order to communicate virtually with other users by uploading content. Uploading content is when an individual uploads data, which is transferred from a computer or phone to another device or the Internet.² A social media site has three main features: firstly, the sharing of information without a specific target.³ Secondly, posting visible information anyone can engage with on the platform regardless of geographical location.⁴ Thirdly, distributing information to users outside of the author's initial connection list.⁵ Social media has proven to be an effective tool in allowing and facilitating communication between individuals on a global scale.⁶ The development of smartphones has played a crucial role in increasing the use of social media platforms. Smartphone features provide easier access for users to upload their content onto these platforms or the Internet.⁷ However, the Internet, especially social media, has provided perpetrators with an effective way to mask themselves behind computer screens to deceive others through online impersonation for malicious purposes, self-gain or even as a pastime. All of these individuals purport to deceive and impersonate others have been commonly referred to as "catfishing".⁸

The effortless process of creating a social media account is one of the main factors attributable to the rise of online impersonation- as an individual only requires a valid email account or an active mobile number to create a social media account.⁹ Even after introducing the Two Factor Authentication process on Facebook, Instagram and X (although it is arguably more challenging to hack into someone else's social media), creating a new social media

¹ A. Petrosyan "Worldwide digital population 2023" (22 May 2023), available at <https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=Worldwide%20digital%20population%202023&text=As%20of%20April%202023%2C%20there,population%2C%20were%20social%20media%20users>, accessed on 13 June 2023.

² L. N. L. Ndyulo *Protecting the right to identity against catfishing* (unpublished LLM thesis, Rhodes University, 2021) at 1.

³ Ibid.

⁴ Ibid.

⁵ Ibid.

⁶ A. Santi "Catfishing": A comparative analysis of the U.S. v. Canadian Catfishing Laws & their limitations' (2019) 44 *Southern Illinois University Law Journal* 73 at 75.

⁷ Ibid.

⁸ Ibid.

⁹ Ndyulo op cit note 2 at 1.

account is still effortless.¹⁰ Online impersonation refers explicitly to cases when a malicious individual uses someone's online identity to gain financial benefits or to harass, intimidate, or threaten their victim. The most common form of online impersonation is identity theft. Identity theft is defined as "the illicit use of another individual's identifying facts (name, date of birth, Identity number, address, telephone number, or other similar information) to perpetrate economic fraud, such as the opening of a bank account, obtaining credit, applying for bank or department store cards, or leasing cars or apartments in the name of another".¹¹ Identity theft is explicitly used in economic-related crimes, whereas online impersonation does not always entail the perpetrator obtaining economic benefits. Online impersonation and identity theft have become easier to commit, as there is a lack of formal identity verification mechanisms when a person creates a social media account. Social media platforms permit users the freedom to portray themselves as they desire online.¹² The lack of regulation is one of the main reasons many active social media accounts are fake or duplicated.¹³

This essay will focus on the crime of online impersonation more broadly, and not the standalone crime of identity theft. As mentioned above, the more common name for online impersonation is catfishing. Catfishing is 'someone who uses false information to cultivate a persona online that does not represent their true identity... [which] commonly involves using stolen or edited photos usually taken from an unwitting third party' or creating a completely fictitious persona.¹⁴ The critical elements of catfishing include creating counter-fit profiles on social media and using these fake accounts for deceptive purposes. While catfishing and online impersonation are generally used as synonyms, catfishing is a broader term that also includes the creation of a fictitious persona through the use of actual individual's photos and videos. Impersonation occurs when the perpetrator copies another person/s on social media using their images to create fake online profiles.¹⁵ People have varying reasons why they catfish; some have malicious intentions, such as fraudulent monetary gain, cyberbullying or humiliating another person, while others have less sinister reasons, such as social validation, loneliness or

¹⁰ E. Boyle "Protecting Your Instagram & Facebook From Hackers: Two-Factor Authentication Explained" *Phorest* June 21 2023, available at : <https://www.phorest.com/blog/two-factor-authentication-explained/#:~:text=Simply%20go%20to%20your%20profile,enable%20it%20for%20your%20account>, accessed on 16 February 2024.

¹¹ V. Basdeo "Criminal and procedural legal challenges of identity theft in the cyber and information age" (2017) *South African Journal of Criminal Justice* 363 at 366.

¹² *Ibid.*

¹³ *Ibid.*

¹⁴ *Santi* op cit note 6 at 76.

¹⁵ *Ibid.*

the enjoyment of digital anonymity.¹⁶ One of the more sinister reasons behind catfishing (namely fraud) has already been regulated by the South African Cybercrimes Act 19 of 2020 (“Cybercrimes Act”)¹⁷.

The Cybercrimes Act was enacted to criminalise the disclosure of harmful data messages and provide interim protection orders to further regulate jurisdiction concerning cybercrimes and to further regulate the powers to investigate cybercrimes, among other reasons.¹⁸ The Cybercrimes Act has criminalised several problematic and dangerous cybercrimes, such as revenge porn and cyberbullying,¹⁹ but has failed to regulate cyber-impersonation, more specifically, catfishing.

My research will argue that the Cybercrimes Act should follow the examples set by several states in the United States of America (USA). The USA states of Oklahoma, California, Texas, and New York have specific legislative provisions that criminalise catfishing as a standalone crime. The USA aims to extend protection to the second victim rather than the direct victim. The second victim in catfishing is the individual being impersonated, and the direct victim is the individual who was made to believe A was person B.²⁰ The rationale behind this approach is to protect a person's name and reputation, as well as prevent harassment.²¹ Protecting an individual's name or reputation ensures that family members, friends, acquaintances, potential romantic partners and even potential employers do not get a false narrative of the individual based on their social media, which could negatively impact their lives outside of social media.²²

Outside of the Cybercrimes Act, South Africa has delictual remedies available for online impersonation and/or catfishing; however, I argue that the USA's example should be followed where both criminal and delictual remedies are available for the cybercrime of catfishing. Unlike the USA, South Africa only offers delictual remedies to the direct victim. South Africa neglects to extend legal protection to the second victim of catfishing, who may have suffered harm due to the deception.²³ Furthermore, South Africa lacks criminalising the crime of

¹⁶ Ibid.

¹⁷ Cybercrimes Act 19 of 2020.

¹⁸ Ibid.

¹⁹ Supra note 17, at s14- s16.

²⁰ Ibid.

²¹ Ibid.

²² A. Derzakarian “The dark side of social media romance: civil recourse for catfishing victims” (2017) 50 *Loyola of Los Angeles Law Review* 741 at 745.

²³ Ibid.

catfishing. This means that no current South African law has effective deterrence mechanisms for the act of catfishing in South Africa. The Cybercrimes Act only provides limited criminal remedies for certain acts related to catfishing and has failed to provide standalone criminal remedies for the impersonation aspect of catfishing.

This research aims to answer how the Cybercrimes Act could effectively regulate catfishing (through amending the Act), taking from the lessons in the USA. Catfishing is a unique cybercrime involving two victims, rendering catfishing a severe offence as its tentacles of harm go further than initially thought. In Part I, I will introduce the concept of catfishing, as well as provide a brief description of the current legal framework in South Africa in relation to catfishing. Part II will consider the history behind the crime of catfishing and how the USA has regulated this cybercrime. Part III will analyse the current South African legal position on catfishing. This section will further discuss the common law crime of fraud, cyber fraud and relevant case law that has dealt with these matters. It will be shown that South Africa's lack of criminalisation of catfishing raises concerns about the available legal remedies for catfishing victims. Part IV will consider the lessons that can be learned from the USA by analysing the relevant provisions from each of the USA states. Part V will provide recommendations of how South Africa could criminalise the act of catfishing with the backdrop of lessons learned from the USA. Lastly, Part VI will provide concluding remarks and recommend an approach to codify catfishing in the Cybercrimes Act.

II WHAT IS CATFISHING?

The term catfish became globally known following a 2010 documentary "Catfish" by Nev Schulman, a man who was a victim of a cyber impersonation scheme himself.²⁴ Schulman created the documentary after discovering that the woman with whom he had a nine-month-long relationship, was a fictitious person.²⁵ The perpetrator was a married woman who had used photographs from a model's account. The model was an innocent third party who had neither consented to the use of her photographs, nor was she aware of this scheme. The model's photographs were used to create a fictitious profile, which Schulman then based his decision on to enter into a relationship with her.²⁶ The perpetrator's husband was the one who inspired

²⁴ Santi op cit note 6 at 76.

²⁵ Ibid.

²⁶ Ibid.

the name Catfish for Schulman's documentary.²⁷ When her husband was interviewed regarding his wife's behaviour, he responded with the following metaphorical explanation:

"They used to take cod from Alaska all the way to China. They'd keep them in vats in the ship. By the time the codfish reached China, the fish was mush and tasteless. So this guy came up with the idea that if you put those cods in these big vats, put some catfish in with them and the catfish would keep the cod agile. And there are those people who are catfish in life. And they keep you on your toes. They keep you guessing, ... they keep you fresh."

Schulman's documentary led to MTV creating the popular series, *Catfish*, in 2012, hosted by Nev Schulman himself.²⁸ The premise behind the series is to assist victims in identifying the individual who deceived them online.²⁹ The series is still ongoing, serving as an indication of how common catfishing is.³⁰

The main aim of catfishing is to deceive another individual.³¹ Catfishing has two primary forms. The first form is where the perpetrator obtains an individual's information without their consent to gain access to their online profiles or impersonate them by creating a fake profile/s.³² The second form occurs when the perpetrator creates an entirely fictitious profile.³³ Catfishing schemes mainly concern themselves with creating a fake persona. The images representing this fake persona are often stolen from a real person's online profile. Therefore, the images used by the fake persona depict a real person.³⁴ There are two main victims in a catfishing scheme: the person being deceived into a romantic relationship (first/direct victim) and the person whose photographs the perpetrator used (second/indirect victim).³⁵ When an impersonating profile uses an individual's identity and photographs on social media, they often do so to create false, harmful and offensive posts that the impersonated individual would never post, and attribute these posts to the impersonated victim.³⁶ Proving that it is necessary to (legally) protect both the first and second victim. Aimee Gonzales, a victim of catfishing, states, 'it's almost worse

²⁷ Ibid.

²⁸ Ibid at 77.

²⁹ Ibid.

³⁰ Ibid.

³¹ Discussed in paragraph 1 above.

³² Ibid at 78.

³³ Ibid.

³⁴ Derzakarian op cit note 22 at 744.

³⁵ Ibid.

³⁶ Ibid.

than stealing someone's name. She actually stole my face. There is nothing more than your face that makes you who you are'.³⁷

The USA's approach stems from the numerous catfishing cases in several states. One of the most well-known and publicised cases of catfishing in the USA was Megan Meier's. In 2006, Megan Meier was a 13-year-old girl who struggled with her weight, self-esteem and depression.³⁸ Megan met Josh Evans, a cute 16-year-old boy, on Myspace, where they developed a relationship. All this occurred while under the supervision of her mother.³⁹ They never met in person or spoke over the phone; their regular interactions were only online.⁴⁰ Before Megan turned 14, the messages from Josh changed. He began accusing her of being mean to her friends, and stated that he was unsure if he wanted to be friends with her.⁴¹ Shortly after, Josh shared some of their private messages with Megan's peers. Her peers began calling her "fat" and a "slut".⁴² In his final message, he told her she was a bad person, that he did not want to be friends anymore, and that the world would be better without her.⁴³ Later that day, Megan hung herself in her closet.⁴⁴ Six weeks after Megan's passing, her parents uncovered that Josh had never existed and their daughter had been catfished under her mother's supervision.⁴⁵ During the investigation, it was discovered that the Myspace profile had been created by Lori Drew, a long-term friend and neighbour of the Meiers.⁴⁶ Drew created the online profile to find out what Megan said about her daughter, Sarah. Drew used a photo of a young boy (without his consent) to attract Megan.⁴⁷ Drew relied on intimate details about Megan's struggles with her weight, depression and self-esteem to bully her.⁴⁸ This case illustrates how easily catfishing can occur and how catfishing is often accompanied by malicious behaviour.⁴⁹

Unfortunately, most of the publicised and reported cases of catfishing relate to instances where the perpetrator defrauded the victims out of their money. Usually, matters of catfishing

³⁷ Ibid.

³⁸ M. Cohen "Angling for justice: Federal Law to reel in Catfishing" (2018-2019) 2 *Journal of Law and Technology at Texas* 51, at 58.

³⁹ Ibid.

⁴⁰ Ibid.

⁴¹ Ibid.

⁴² Ibid.

⁴³ Ibid.

⁴⁴ Ibid.

⁴⁵ Ibid at 59.

⁴⁶ Ibid.

⁴⁷ Ibid.

⁴⁸ Ibid.

⁴⁹ Ibid.

negatively impact an individual's personal life. One South African case (where the victim was defrauded out of their money) was of Louise Heyins from Cape Town, who was lonely and found romance online with a man she thought was American.⁵⁰ The two individuals chatted online for six months before the catfish started asking for money. Ms Heyins used Moneygram and Western Union to transfer money to him.⁵¹ Ms Heyins transferred R600,000 to cover the costs of his apparent children's medical expenses. Ms Heyins willingly did this, as she was aware of the emotional impact of losing a child. After she had given him roughly R800,000.00, Ms Heyins never heard from her catfisher again.⁵² This serving as a perfect example of a catfisher utilising personal facts to coerce their victim.⁵³

Another South African case involved Anita (alias name), a widow, who believed she found love on a dating app, Tinder. Anita met Ramstein van Holt.⁵⁴ After about four months, Van Holt started requesting money for various reasons. During their nine-month relationship, Anita transferred R500,000, which was everything she owned.⁵⁵ She had no idea that the photos Van Holt sent her and used on his profile were photos of a Greek politician and that she was to become a victim of an online romance scam.⁵⁶ Anita discovered she was speaking to a homeless person who a syndicate in South Africa had set up to be part of the deception.⁵⁷ These catfishing stories are examples of why catfishing should be regulated through legislation globally and, more specifically, in South Africa.

III THE SOUTH AFRICAN POSITION ON CATFISHING

On the face of it, South Africa's legal framework does provide legal remedies in cases of catfishing; and these will be assessed to determine whether the remedies are sufficient to deter the act of catfishing. The remedies that will be evaluated specifically include: the law of delict, common law fraud and cyberfraud, the Cybercrimes Act, and *Crimen iniuria*.

(a) The law of Delict

Although it is beyond the scope of this research, it is worth mentioning that even though South Africa lacks the criminalisation of catfishing, South Africa does have delictual remedies to

⁵⁰ K. Geldenhuys "Scammed out of love" (June 2020) *Community-based Safety & Security Magazine* at 26.

⁵¹ Ibid.

⁵² Ibid.

⁵³ Ibid.

⁵⁴ Ibid at 24.

⁵⁵ Ibid.

⁵⁶ Ibid.

⁵⁷ Ibid.

assist victims of catfishing. South Africa's law of delict protects an innocent third party in catfishing cases, where the catfish used the individual's photographs and likeness to create a false social media account. Catfishing is an infringement of the right to identity by falsification, as the catfish uses the second victim's image or photos to create a false persona to trick the first victim.⁵⁸ Misusing the victim's image and the catfish's conduct, creates a false impression of the victim to the public.⁵⁹ Catfishing is also a misappropriation of identity, as it involves the unauthorised appropriation of one's image or likeness for commercial gain; however, this only applies where the catfish's sole purpose is to commit fraud using an unknowing victim's image.⁶⁰

The South African law of delict protects a person's rights to dignity and identity, which are fundamental rights enshrined in the Constitution of the Republic of South Africa, 1996.⁶¹ Using the victim's image in a reprehensible manner injures their dignity, and identity and dignity are often closely linked to each other, especially in South African law.⁶² The long-standing academic debate of whether the misappropriation of a person's image constitutes an identity or privacy infringement was settled in *Grütter v Lombard*.⁶³ The court held that misappropriation of a person's image is an identity concern in terms of the law of delict. Claiming for delictual remedies often involves tedious processes when litigating, and the monetary compensation a victim could gain for the infringement of personality is minuscule, as was seen in the case in *Wells v Atoll Media (Pty) Ltd (Wells case)*.⁶⁴ Compensation, as a sanction by itself, does not serve as a strong enough incentive for catfishing criminals to avoid performing the act of catfishing. The damage the catfish causes is more significant than the monetary compensation they would have to pay if the victims were to take them to court. Albeit a concise summary of South Africa's delictual remedies to deal with catfishing, the lack of criminalisation hinders the deterrence of the act.

⁵⁸ Ndyulo op cit note 2 at 9.

⁵⁹ Ibid.

⁶⁰ Ibid.

⁶¹ Constitution of the Republic of South Africa, 1996, s10.

⁶² Ndyulo op cit note 2 at 10.

⁶³ *Grütter v Lombard* 2007 4 SA 89 (SCA).

⁶⁴ The case of *Wells v Atoll Media (Pty) Ltd* [2010] 4 All SA 548 (WCC) will be discussed later at page 14 below. In this case, a minor child was defamed in a magazine. She was bullied in school. The court found that R10,000.00 compensation was enough.

(b) Common law Fraud

The common-law offence of fraud could arguably be used in certain instances of catfishing. The common-law offence of fraud is defined as 'unlawfully making, with the intention to defraud, a misrepresentation which causes actual prejudice or which is potentially prejudicial to another'.⁶⁵ Fraud is the common-law crime of the liar, cheat or confidence trickster; it seeks to punish those who use deceptive means to obtain property or other advantages from another person.⁶⁶ There are four essential elements to fraud, namely, unlawfulness, misrepresentation, prejudice and intention.⁶⁷ Prejudice is a "preconceived opinion that is not based on reason or actual experience".⁶⁸ Prejudice can be pecuniary (monetary compensation) or non-pecuniary.⁶⁹ The main element of fraud relevant to catfishing is the element of prejudice. A mere lie does not bring about prejudice; the crime is only committed if the lie brings about some form of harm to another person.⁷⁰ The fraudulent act can bring about proprietary (ownership) or non-proprietary harm, often prejudice associated with a person's reputation or dignity.⁷¹ An example is when person A impersonates person B, and person A writes an exam on behalf of B.⁷² Furthermore, fraud victims need not suffer real or actual prejudice; it is sufficient where there is merely the potential, or risk, of suffering prejudice.⁷³ Potential prejudice is where there was a misrepresentation, and when looked at objectively, it must involve the risk of prejudice, be it proprietary or non-proprietary.⁷⁴ It is not essential for potential harm to be suffered by the person to whom the misrepresentation is made; it is sufficient if a third person or the government would have been prejudiced by such misrepresentation.⁷⁵

(c) The Cybercrimes Act

Snail ka Mtuze notes that South Africa has far-reaching remedies for the common-law offence of fraud. However, the common-law position is insufficient for cybercrimes such as cyber-

⁶⁵ J. Burchell *Principles of Criminal Law* 5 ed (2016) 742.

⁶⁶ Ibid.

⁶⁷ Ibid at 744.

⁶⁸ Ibid.

⁶⁹ Ibid.

⁷⁰ Ibid at 749.

⁷¹ Ibid.

⁷² Ibid.

⁷³ Ibid at 742.

⁷⁴ Ibid at 751.

⁷⁵ Ibid.

fraud that entails defamation, indecency, theft, forgery and malicious damage to property.⁷⁶ Although Snail acknowledges that South Africa's case law has slowly developed around these issues, it still has a long way to go⁷⁷. The case of *Okundu v S*⁷⁸ centred around cyber-fraud where the court applied provisions of the Cybercrimes Act and the Electronic Communications and Transactions Act 25 of 2002 (the ECTA)⁷⁹ to convict the accused. In *Okundu*, the appellant, had been convicted for unlawfully gaining access to confidential banking information of various persons to whom banking cards were issued, specifically, the information encoded on the magnetic strips of these original cards.⁸⁰ The appellant had neither the authority nor the consent of the lawful cardholders or the bank to access the information. In this case, the court held that the appellant had committed an offence in terms of s86(4) of the ECTA, whose equivalent is s8 of the Cybercrimes Act⁸¹. In applying s8 of the Cybercrime Act, the court convicted the appellant of unlawfully making misrepresentations to the banks intending to defraud them, causing prejudice to them and/or the lawful cardholders.⁸²

As stated in the *Okundu* case, cyber-fraud is regulated by the Cybercrimes Act, along with cyber forgery and uttering, which are crimes intrinsic to catfishing, precisely where fraud is involved. Cyberfraud often occurs in phishing and pharming scams.⁸³ Phishing scams involve an email fraud method in which the perpetrator sends out "legitimate-looking" emails to gather recipients' personal and financial information.⁸⁴ Pharming occurs when victims are directed to a fake or bogus website that tricks them into supplying personal information such as credit card numbers and passwords.⁸⁵ S8 of the Cybercrimes Act covers these aspects of catfishing, where a catfish misrepresents an individual to obtain monetary benefits from the act. S8 of the Cybercrimes Act 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 ... or interference with a computer data storage medium or a computer

⁷⁶ S. Snail ka Mtuz "The Convergence of Legislation on Cybercrime and Data Protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013" *OBITER* (2022) at 539.

⁷⁷ *Ibid.*

⁷⁸ *Okundu v S* (CA&R117/16) [2016] ZAECGHC 131.

⁷⁹ Electronic Communications and Transactions Act 25 of 2002.

⁸⁰ Mtuz op cit note 76 at 541.

⁸¹ *Ibid.*

⁸² *Ibid.*

⁸³ S. Papadopoulos & S. Snail S (eds) *Cyberlaw @ SA: The law of the Internet in South Africa* 4th ed (2022) Van Schaick Publishers: Pretoria at 553.

⁸⁴ *Ibid.*

⁸⁵ *Ibid.*

system ... which causes actual or potential prejudice to another person, is guilty of the offence of cyber fraud'.⁸⁶

S19(6)(a) of the Cybercrimes Act makes direct imprisonment (with or without a fine) a mandatory sentence where a person is convicted of any of the offences provided for in s8, and if the offence was committed by the person (or in collusion or with the assistance of another person) who:

"as part of their duties, functions or lawful authority was in charge of, in control of, or had access to data, a computer programme, a computer data storage medium or a computer system belonging to another person in respect of which the offence in question was committed".⁸⁷

Catfishing is a crime that does not always comprise of fraud but always entails impersonation. Therefore, I submit that s8 of the Cybercrimes Act offers anyone who was catfished and subjected to fraud for the catfish to gain monetary benefit a legal remedy. However, s8 of the Cybercrimes Act is inadequate to address the impersonation aspects in catfishing crimes.

Sections 14 and 15 of the Cybercrimes Act, could potentially be relevant for catfishing perpetrators.⁸⁸ s14 of the Cybercrimes Act creates an offence if a person discloses, by means of an electronic communications service, a data message to a person, group of persons or the general public with the intention to incite damage to property that belongs to, or violence against, a person or a group of persons.⁸⁹ s15 creates an offence where a person unlawfully and intentionally discloses a data message that threatens a person or a related person with damage to property belonging to that person or a related person.⁹⁰ What is unique about s15 of the Cybercrimes Act is that a mere threat of damage to property or violence is punishable as an offence.⁹¹ s19(7) of the Cybercrimes Act states that where a person contravenes s14 or s15, such a person is liable on convictions to a fine or imprisonment for a period not exceeding three years or to both a fine and such imprisonment.⁹²

These provisions, therefore, protect individuals from threats of harm, damage to property or threats of violence emanating from data messages (such as emails, messages sent on social

⁸⁶ Supra note 16 s8.

⁸⁷ Snail op cit note 83 at 554.

⁸⁸ Supra note 16, s14 and s15.

⁸⁹ Ibid at 551.

⁹⁰ Ibid.

⁹¹ Ibid.

⁹² Ibid at 554.

media and so forth). However, not all direct or indirect catfishing victims are subject to threats of violence or damage to property. Direct catfishing victims are more commonly subjected to these types of threats by the catfish during their online interactions. Simultaneously, indirect catfishing victims are usually subjected to threats of harm when the indirect victim approaches the catfish using their photos or likeness for their fake persona. s14 and s15 of the Cybercrimes Act only extends protection to individuals (direct victims) where there is a mere aspect of harm that could be caused by catfishing, rendering sections 14 and 15 of the Cybercrimes Act inadequate to address all catfishing cases.

Lastly, s16 of the Cybercrimes Act creates an offence in relation to the disclosure of data messages of an intimate image nature (colloquially known as "revenge porn"). s16 of the Act makes it an offence where a person unlawfully and intentionally discloses, by means of an electronic communications service, a data message of an intimate image of a person without the consent of such a person.⁹³ S19(7) of the Cybercrimes Act provides that anyone contravening s16 is liable on conviction to a fine or imprisonment for a period not exceeding three years or to a fine and imprisonment not exceeding three years.⁹⁴ This provision aims to protect individuals from the threat of the disclosure of intimate images of themselves. This provision could protect both the direct and indirect catfishing victims. The direct victim can be protected from the catfish sharing intimate images they shared during their online romantic relationship, and the indirect victim can be protected from the catfish using any intimate images of the indirect victim that they found online. S16 of the Cybercrimes Act further offers indirect victims protection from the catfish when the catfish uses or creates intimate images of the victim through the use of Artificial Intelligence (specifically, "Deepfakes"). However, s16 of the Cybercrimes Act will only protect direct and indirect victims where intimate images were shared during the catfishing. It does not cater to the impersonation aspect of the crime. Thus rendering s16 of the Cybercrimes Act inadequate to address catfishing holistically.

While South Africa's current legal framework provides protection and remedies for catfishing, which involves fraud, threats of harm to damage to property, or threats of violence emanating from data messages, and threats of the disclosure of intimate images and delictual remedies, these laws leave many victims unaided and unsatisfied, for the following reasons. Firstly, a delictual claim for harm emanating from an image right and/or personality infringement does not adequately compensate the victim, whose photographs and likeness were

⁹³ Ibid.

⁹⁴ Mtuz op cit note 76 at 555.

used in the catfishing scheme. Often, the monetary compensation awarded by the courts in cases where a person's image was used without their consent appears to omit the prejudice caused to these victims, which has become well-known and established in delictual cases.

In the *Wells* case, a 12-year-old girl's bikini photo was published on the cover of a surfer's magazine, where the words "pure filth" was written alongside her picture.⁹⁵ The 12-year-old girl was vehemently bullied by peers and individuals outside her school. She lived in a small community in Port Elizabeth, making it easy for her to be identified as the girl in the photograph.⁹⁶ Despite her suffering, the court awarded her R10 000 in damages, along with costs.⁹⁷ This is bitterly shy of the R500,000 her mother had originally wanted to claim for her daughter.⁹⁸ Additionally, the psychological and reputational harm she suffered is the sort that will haunt her for life. The court held that "generosity of amount is perhaps less important than the principle that damages have been awarded because the plaintiff has been wronged."⁹⁹ Although this reasoning can be appreciated, the issue with delictual damages in South African courts is that the victims will never feel fully "compensated" for the emotional damages incurred.

Secondly, victims who have been conned into falling in love with the catfish through fraud will have no legal recourse where the victim suffered psychological, emotional, or monetary loss, especially small monetary claims. The amount of time, money and effort incurred for a South African Police Service (SAPS) investigation (especially for a small claim) from a catfishing victim is unlikely to be taken seriously, especially considering the oversaturation of crimes SAPS has to deal with daily.¹⁰⁰ Many individuals scammed out of thousands of rands may not find it worthwhile or may not have the funds to hunt down their catfishers and follow them to court. Fortunately, Anita and Ms Heyins, who were conned out of hundreds of thousands of rands by their catfishers, were financially able to hire a private investigator to track down the catfishing criminals, which ultimately led to their arrests.¹⁰¹ This highlights the need for the act of catfishing to be criminalised, which would assist in incentivising victims and law enforcement to bring catfishers to justice.

⁹⁵ Ibid para 9.

⁹⁶ Ibid para 12.

⁹⁷ Ibid para 51.

⁹⁸ Ibid para 1.

⁹⁹ Ibid para 50.

¹⁰⁰ S. Schrieber "Unresolved cases: As crime increases, SAPS continues to lose detectives" *Times Live* 30 June 2023.

¹⁰¹ Supra note 50, at 27.

The criminal offence of fraud potentially offers the impersonated catfishing victim claims for non-pecuniary/non-proprietary reasons for reputational harm as a third party. Most catfishing victims, who were not scammed out of money, would find it difficult to claim emotional damage. The issue with reputational harm (also known as defamation of character) claims is that the courts award abysmal amounts to compensate the victims of reputational harm. Another example, aside from the *Wells* case, is the case of *Isparta v Richter and Another*.¹⁰² In this case, a recently divorced man posted on Facebook that his ex-wife was a bad mother and allowed an inappropriate relationship between her stepson and their daughter.¹⁰³ The court held this to be a defamation of character but only awarded the ex-wife R40,000 in damages.¹⁰⁴ The awards for defamation cases are abysmal, as pointed out by Harms JA in *Mogale and Others v Seima*,¹⁰⁵ who argued that "awards generally do not serve a punitive function and are, generally, not generous".¹⁰⁶ This confirms that s14, s15 and s16 of the Cybercrimes Act¹⁰⁷ only criminalise certain aspects related to the crime of catfishing but does not adequately address the problem of impersonation inherent to the crime of catfishing. These sections of the Cybercrimes Act, although useful in some cases of catfishing, would not be applicable to all cases and are, therefore, inadequate in addressing the issue of catfishing in South Africa.

(d) *Crimen iniuria*

The only alternative criminal remedy available in catfishing cases would be the criminal law remedy of *crimen iniuria*.¹⁰⁸ *Crimen iniuria* definition is "unlawfully and intentionally impairing the dignity and privacy of another person".¹⁰⁹ *Crimen iniuria* aims to shield persons from having their dignity impaired by words or conduct that are insulting, contemptuous or disrespectful.¹¹⁰ *Crimen iniuria* differs from the delictual remedy of defamation, which involves the communication of the insults and focuses on the harm caused to the dignity of the victim only.¹¹¹ Such violations of dignity constitute a civil wrong and can be redressed through

¹⁰² *Isparta v Richter and Another* [2013] JOL 30782 (GNP).

¹⁰³ *Ibid* para 8-12.

¹⁰⁴ *Ibid* para 41.

¹⁰⁵ *Mogale and Others v Seima* 2008 (5) SA 637 (SCA) at paras [9] to [12] and [18].

¹⁰⁶ *Ibid*.

¹⁰⁷ *Supra* note 26 at s14,15 and s16.

¹⁰⁸ Burchell *op cit* note 64 at 648.

¹⁰⁹ *Ibid* at 648

¹¹⁰ *Ibid*.

¹¹¹ *Ibid*.

an action for damages.¹¹² However, there are insults to dignity that are so gross they evoke public outrage and call for public denunciation through criminal law.¹¹³ It is in these instances where the *crimen iniuria* finds application.

The essential elements of *crimen iniuria* are unlawfulness, the impairment of dignity, and intention.¹¹⁴ The first element is unlawfulness, which objectively determines whether a person's dignity has been impaired.¹¹⁵ The basis for judging the gravity of the infringement on an individual's dignity is largely based on the courts' conception of *boni mores* (good morals).¹¹⁶ Some factors determining the seriousness of the impairment of dignity are based on age, gender, sexual impropriety, unfair discrimination, persistence, publicity, the public interest and the nature of the act.¹¹⁷ Age and gender are often factors where the catfish uses online impersonation as a means to groom their underaged victim/s. The second element assesses the seriousness of the impairment to dignity. To determine whether the individual's dignity was impaired, one must not look at the sensibility of the complainant nor the hypersensitivity of the individual but rather that of a reasonable person.¹¹⁸ Examples where catfishing would constitute an impairment of dignity would be; "grooming", inducing engagement and intercourse by fraud, abusive or insulting or degrading communications, or the invasion of privacy.¹¹⁹ Grooming of an underaged victim or the vulgar abuse, insult or humiliation of an individual through catfishing could be a factor in the impairment of dignity.¹²⁰ However, the use of abusive, insulting or degrading communication is often difficult to prove. This was shown in the case of *S v Sharp*,¹²¹ where a policewoman was called a "bitch" in front of her colleagues by a citizen. The court found that this degrading comment was not deemed to be an impairment of her dignity. This can be problematic in catfishing cases, as many of the indirect victims' reputations may be affected by degrading comments made by the catfish online. The last element is intention, specifically intention in the form of *dolus eventualis*.¹²² *Dolus eventualis* is defined as the concept where "the perpetrator must have either known or foreseen that the conduct might unlawfully impair the victim's dignity".¹²³ Therefore, if a catfisher grooms an

¹¹² Ibid at 649.

¹¹³ Ibid.

¹¹⁴ Ibid at 650.

¹¹⁵ Ibid.

¹¹⁶ Ibid at 651.

¹¹⁷ Ibid at 651-653.

¹¹⁸ Ibid at 654.

¹¹⁹ Ibid at 655-657.

¹²⁰ Ibid at 656.

¹²¹ *S v Sharp* 2002 (1) SACR 360 (CKHC)

¹²² Burchell op cit note 64 at 658.

¹²³ Ibid.

underaged victim, or if the catfish publishes abusive, insulting or degrading communications on an online platform about either the direct or indirect victim of catfishing- they could be held criminally liable in terms of the *crimen iniuria*.

Martin explores the use of *crimen iniuria* as a remedy for image-based sexual abuse victims.¹²⁴ He assesses the case of *S v Brereton*,¹²⁵ where a maize farmer caught a number of women stealing maize from his farm. When he caught these women, he vengefully removed the top part of their clothing, exposing them from the waist upwards, and male farm workers witnessed this demonstration¹²⁶. The charges brought against the farmer were assault, criminal defamation and *crimen iniuria*.¹²⁷ The court expressed that the proper thing to do was charge the defendant with the more serious of the three charges, *crimen iniuria*.¹²⁸ *S v Brereton* is an example of where an action that sparks a level of outrage will require a proportionately equivalent punishment.¹²⁹ As shown, *crimen iniuria* provides victims of catfishing a remedy; however, it is highly unlikely that catfishing cases would "spark a level of outrage" that is required for the *crimen iniuria*. The *crimen iniuria* remedy is, therefore, generally "out of reach" for victims of catfishing and ineffective in addressing the issue of catfishing in South Africa.

It is evident that South Africa's legal framework does provide remedies for catfishing victims in the law of in delict, certain sections of the Cybercrimes Act and through the criminal law remedy of *crimen iniuria*; however, there needs to be stronger regulations that will act as deterrence for potential catfishers. A criminal conviction speaks admirably to the gravity of catfishing, with the purposes of punishment: retribution, prevention and deterrence,¹³⁰ and a stronger incentive for both catfishing victims to institute a claim against the catfish. The predominant issue in catfishing is not always an intention to harm the victim; rather, the catfish will always intend to deceive third parties through impersonation.¹³¹ It is thus worthwhile to consider how several states in the USA have criminalised online impersonation as an

¹²⁴ B. N. Martin "Mixing old and new wisdom for the protection of image based sexual abuse victims" (2022) *South African Journal of Criminal Justice* 307 at 309.

¹²⁵ *S v Brereton* 1971 (1) SA 489 (RA).

¹²⁶ Martin op cit note 123 at 326.

¹²⁷ Ibid.

¹²⁸ Ibid at 326.

¹²⁹ Ibid.

¹³⁰ Ibid at 309.

¹³¹ Ndyulo op cit note 2 at 119.

independent offence from fraud, specifically cyber fraud, and what lessons South African law can learn therefrom.

IV CATFISHING IN THE USA

The USA's legal system is a dual system divided into federal and State law.¹³² The US Constitution establishes a federal government, which is similar to the South African national government.¹³³ Each of the fifty states has its own State Constitutions, empowering individual State governments to legislate for their State while assigning certain powers to the federal government.¹³⁴ The legal areas and questions not dealt with in federal law are dealt with in their state law.¹³⁵ It should be noted that catfishing is not dealt with by federal law but rather at State government level.¹³⁶

Where federal law and State law intersect, federal law takes preference over State law, as confirmed in the supremacy clause.¹³⁷ The USA's supremacy clause gives rise to the doctrine of pre-emption, which provides that if State law conflates with federal law, then State law must give way to the application of federal law.¹³⁸ Federal law sets the standard, and States can decide to improve the standards set by federal law by enacting more specific laws.¹³⁹ Several USA states have criminalised catfishing through identity theft statutes, and many explicitly criminalise online impersonation through specific statutes dedicated to online impersonation as opposed to identity theft alone.¹⁴⁰ In turn, several states in the USA will be analysed to assess how they specifically criminalise the act of catfishing. The USA's online impersonation statutes primarily incorporate the following key elements: (a) impersonation without the victim's consent, (b) through an electronic communication channel such as social networking sites, emails, text messages, amongst others, and (c) the perpetrator must act with the intention to harm, intimidate, threaten or defraud.¹⁴¹ It is worth noting that the USA classifies crimes into two broad categories, namely felonies or misdemeanours. A felony is a more serious crime than

¹³² Ibid at 13.

¹³³ Ibid.

¹³⁴ Ibid.

¹³⁵ Ibid.

¹³⁶ Ibid.

¹³⁷ Ibid.

¹³⁸ Ibid.

¹³⁹ Ibid.

¹⁴⁰ Santi op cit note 6, at 86.

¹⁴¹ K. Clanton "We are not who we pretend to be: ODR alternatives to online impersonation statutes" (2014) 16 *Cardozo Journal of Conflict Resolution* 323 at 5.

a misdemeanour and carries much higher penalties, such as long-term jail sentencing.¹⁴² The potential sentence usually determines the classification of a crime.¹⁴³ Most states in the USA define felonies as crimes punishable by death or imprisonment for more than one year, while all other less serious crimes are considered misdemeanours.¹⁴⁴ Misdemeanours are crimes punishable by other sentences aside from death and will either be punished by a fine, imprisonment or both.¹⁴⁵ The following States, Oklahoma, California, Texas, and New York, have criminalised online impersonation as an independent criminal offence from fraud. Each of these States will be discussed below and used to analyse how they have criminalised catfishing.

(a) New York

The New York statute was amended to incorporate Internet impersonation in March 2007 in the New York Penal Code (S.4053, 2007-2008 Reg. Sess. N.Y. 2008).¹⁴⁶ The New York online impersonation law is known as The New York Penal Code, which criminalises catfishing through criminal impersonation statutes that distinguish between two degrees of criminal impersonation.¹⁴⁷ Criminal impersonation in the first degree is considered a felony (N.Y. Penal Law §190.26). This section specifically targets online impersonation of law enforcement officers and medical and dental care professionals.¹⁴⁸ Criminal impersonation in the second degree is considered to be a misdemeanour.¹⁴⁹ This section targets the online impersonation of the general public.¹⁵⁰ For online impersonation to rise to the second degree, the person needs to 'impersonate another by communication by Internet website or electronic means with the intent to obtain a benefit or injure or defraud another'.¹⁵¹ Here, victims are required to prove the element of intent for the catfishing crime to rise to the level of criminal impersonation in the second degree.¹⁵² Online impersonation only constitutes a misdemeanour punishable by imprisonment for up to a year and a fine of up to \$10,000.¹⁵³ By the plain language of the New York Penal Code, the law applies to any person or entity impersonating another person on the

¹⁴² J. M. Pollock *Criminal Law* 10th ed (2012) at 27.

¹⁴³ D. S. Broyles *Criminal Law in the USA* (2015) at para 260.

¹⁴⁴ *Ibid.*

¹⁴⁵ *Clanton op cit* note 141 at 27.

¹⁴⁶ *Ibid* at 87.

¹⁴⁷ *Ibid.*

¹⁴⁸ *Ibid.*

¹⁴⁹ *Ibid* (§ 190.25).

¹⁵⁰ *Ibid.*

¹⁵¹ *Ibid.*

¹⁵² *Ibid.*

¹⁵³ *Clanton op cit* note 141 at 8.

Internet.¹⁵⁴ This new law intends to deter the enormous amount of misrepresentation cases that have occurred in the USA through the use of the Internet.¹⁵⁵ The only issue with the New York Penal Code is that it still contains an element parallel to fraud in South Africa, the element of intent to obtain a benefit, or injure or defraud another".¹⁵⁶ As with its South African counterpart, this element may be difficult to prove as not all catfishing cases involve a perpetrator who intends to benefit monetarily through injuring the direct victim financially.

(b) California

California's statute imposes both criminal and civil liability for online impersonation.¹⁵⁷ The statute aimed at expanding the current impersonation statute to include impersonation done on the Internet website or through any other electronic means such as email.¹⁵⁸ The California Penal Code (Cal. Penal Code) §528.5 provides that 'any person who knowingly and without consent credibly impersonates another actual person through or on an Internet website or by other electronic means for purposes of harming, intimidating, threatening or defrauding another person is guilty of a public offence'.¹⁵⁹ The statute goes further to state that "in addition to any other civil remedy available, a person who suffers damages or loss by reason of a violation [of the statute] may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief".¹⁶⁰ Subdivision (a) requires the perpetrator to "credibly" impersonate another person on the Internet website or by other electronic means with the intent to harm, intimidate, threaten or defraud another person.¹⁶¹ A credible impersonation, as defined by subdivision (b), occurs when "another person would reasonably believe, or did reasonably believe, that the defendant was or is the person who was impersonated".¹⁶² A credible impersonation based on subdivisions (a) and (b) constitutes a misdemeanour or offence punishable by a fine not exceeding \$1000, or imprisonment not to exceed one year, or both a fine and imprisonment.¹⁶³ California's statute is considered to be the most sophisticated statute to govern the issue of catfishing or, more broadly, identity theft.¹⁶⁴

¹⁵⁴ Ibid.

¹⁵⁵ Ibid.

¹⁵⁶ Santi op cit not 6, at 87.

¹⁵⁷ Ndyulo op cit note 2 at 70.

¹⁵⁸ Clanton op cit note 141 at 6.

¹⁵⁹ Ibid.

¹⁶⁰ Ibid.

¹⁶¹ Clanton op cit note 141 at 6.

¹⁶² Ibid.

¹⁶³ Ibid.

¹⁶⁴ Santi op cit note 6 at 88.

This combination of civil and criminal liability is said to effectively deter and punish catfishing while also providing equitable redress to the victims.¹⁶⁵

California's combination of criminal and civil liability for catfishing showcases how serious the offence is and serves as a strong deterrence.¹⁶⁶ Furthermore, the California statute includes harms that other states have not considered.¹⁶⁷ Some of the harms that other states have not yet considered that California prohibits "impersonat[ing] another person through or on an Internet Website or by other electronic means for purposes of harming, intimidating, threatening, or defrauding persons".¹⁶⁸ The scope of the California Penal Code is wider than the current scope of fraud in South Africa, as it includes the elements of intent to harm, intimidate and threaten. It expressly allows an individual to lay a criminal charge and claim delictual remedies from the catfish. This would mean that even if a catfish is rendered "judgment proof" when held liable under the civil portion of the statute, the catfish may still be held liable under the criminal portion of the statute.¹⁶⁹ The California Penal Code, is similar to the New York Penal Code; however, it limits ways in which victims are able to prove that the catfisher intended to harm, intimidate, threaten or defraud the victim.¹⁷⁰ California's statute is limited to the impersonation of actual persons, which means that certain catfishing victims, such as juristic persons, will be left without legal recourse.¹⁷¹

(c) Oklahoma

Oklahoma has established the Catfishing Liability Act, which specifically addresses online catfishing.¹⁷² The Act provides that

"any person who knowingly uses another's name, voice, signature, photograph or likeness through social media to create a false identity without such persons consent... for the purposes of harming, intimidating, threatening or defrauding such person shall be liable for online impersonation and liable for any damages sustained by the person or persons injured as a result thereof...".¹⁷³

¹⁶⁵ Ndyulo op cit note 2 at 70.

¹⁶⁶ Ibid.

¹⁶⁷ Santi op cit note 6, at 88.

¹⁶⁸ Ibid at 89.

¹⁶⁹ Cohen supra note 37 at 71.

¹⁷⁰ Ibid.

¹⁷¹ Cohen op cit note 37 at 71.

¹⁷² Ndyulo op cit note 2 at 119.

¹⁷³ Cohen op cit note 37 at 69. (OKLA. STAT. tit. 12 §1450 (2017))

The statute shows that the protection offered against catfishing in Oklahoma is only available to victims where the purpose of the catfishing was to defraud, intimidate, threaten or harm the plaintiff.¹⁷⁴ It specifically excludes liability where the sole purpose of the online impersonation is satire or parody, as provided for under §1450. Although the courts in Oklahoma have not been able to interpret this Act, it is submitted that both the direct and indirect victims of catfishing could claim that they have suffered emotional harm from the catfishing scheme.¹⁷⁵ Catfishing victims in Oklahoma may rely on both this Act and any other legal remedy to seek recourse from the catfish who used their identity in a catfishing scheme. Therefore, under the Catfishing Liability Act, the indirect victim would have legal recourse in this manner.¹⁷⁶ §1450F of the Catfishing Liability Act states that the legal remedies in the Act are cumulative and additional to other available legal remedies.¹⁷⁷ However, this Act is narrowly limited to social media, which is problematic as it may limit the statute's ability to keep up with and be applicable to new technologies.¹⁷⁸ Thus, this statute falls short compared to the Texas Penal Code, which provides redress for victims who were not harmed, defrauded, intimidated or threatened by the catfish.

(d) Texas

The Texas Penal Code §33.07 (the Code) was amended in 2011 from "Online Harassment" to "Online Impersonation".¹⁷⁹ The Code states that a perpetrator commits online impersonation when the catfish, without obtaining another individual's "consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person to create a fictitious profile or post messages on a social networking site or another Internet webpage".¹⁸⁰ Under the Code, online impersonation can constitute either a misdemeanour or felony, depending on whether the perpetrator acted with or without malicious intent.¹⁸¹ The conduct enumerated in subsection (a) constitutes a third-degree felony where a conviction can constitute up to 10 years imprisonment and or a fine of up to \$10,000, whereas subsection (b) sets out conduct that is sufficient to constitute a misdemeanour, which is punishable by up to one year in prison, and or a fine of up to \$4,000.¹⁸² Subsection (a) creates a felony where one uses the

¹⁷⁴ Ndyulo op cit note 2 at 119.

¹⁷⁵ Ibid at 119.

¹⁷⁶ Ibid.

¹⁷⁷ Cohen op cit note 37 at 69.

¹⁷⁸ Cohen op cit note 37 at 70.

¹⁷⁹ Clanton op cit note 141 at 7.

¹⁸⁰ Santi op cit note 6 at 89 and (TEX. PENAL CODE §33.07 (a)(1)(2)(2011)).

¹⁸¹ Clanton op cit note 141 at 7.

¹⁸² Ibid at 7.

name or persona of another person, and it does not have to be an identical match.¹⁸³ Subsection (a) is, therefore, broad enough to be applied in cases where the victim's persona or photograph is used to create a social media profile, even when the profile is created under a fake name.¹⁸⁴ The main difference between subsections (a) and (b) is mainly that the misdemeanor offence under subsection (b) only required the perpetrator to engage in the distribution of another individual's identifying information, whereas the felony charge provided for under subsection (a) required the creation of a web presence using the victim's persona or name (it can also be a fake name as previously stated).¹⁸⁵ Under subsection (b), the misdemeanor does not require the perpetrator to act with the intent to intimidate or threaten; it only requires that the perpetrator attempts to harm or defraud the victim.¹⁸⁶

The Code provides a higher degree of protection in that it prohibits situations in which the perpetrator is not proactively engaging in harmful conduct by faking someone else's identity but instead causes someone else to mistakenly start communication with a non-consenting party and thereby attempting to use the acts of innocent third parties to harass the victim.¹⁸⁷ However, it is important to mention that intent on the part of the catfish must still be shown, which can be difficult to prove when the victim cannot show that there was purpose to harm, defraud, intimidate, or threaten.¹⁸⁸ Another issue with this Code is that it does not provide the option for a civil and criminal remedy, such as in California.

(e) Arizona

Arizona has criminalised online impersonation through its identity theft statute.¹⁸⁹ The statute provides that a perpetrator is guilty of online identity theft when they knowingly take or use any personal identity information from another person, which would include a real or fictitious person or entity, without the consent of that person or entity and this is whether or not the person or entity actually suffers any economic loss as a result of such an offence.¹⁹⁰ The section provides that:

"A person commits taking the identity of another person or entity if the person knowingly takes, purchases, manufactures, records, possesses or uses any personal identifying information or

¹⁸³ Ibid at 7.

¹⁸⁴ Ibid at 7.

¹⁸⁵ Ibid at 7.

¹⁸⁶ Ibid at 7.

¹⁸⁷ Santi op cit note 6 at 89.

¹⁸⁸ Ibid at 89.

¹⁸⁹ Ibid at 88.

¹⁹⁰ Ibid at 88 and(ARIZ. REV.STAT.ANN §13 (2008)).

entity identifying information of another person or entity, including a real or fictitious person or entity, without the consent of that other person or entity, with the intent to obtain or use the other person's or entity's identity for any unlawful purpose or to cause loss to a person or entity whether or not the person or entity actually suffers any economic loss as a result of the offense, or with the intent to obtain or continue employment."

Even though Arizona's statute does not explicitly mention "online impersonation", it is implied through the statute's use of broad language and can be applied to catfishing cases where the statute's elemental requirements are met.¹⁹¹ This form of impersonation is regarded as a class four (4) felony, which is an offence that could result in imprisonment of between one and three years.¹⁹² This statute does not require any form of intent to harm, intimidate, threaten or defraud another person- as it only requires "intent to obtain or use the other person's or entity's identity for any unlawful purpose or to cause loss to a person or entity whether or not the person or entity actually suffers any economic loss as a result of the offense, or with the intent to obtain or continue employment".¹⁹³ Unlike the other Codes, the identity theft statute only requires proof that the perpetrator had the intent to impersonate for an unlawful purpose or to cause some form of economic loss. However, Arizona fails to allow the option for both a civil and criminal remedy for the catfishing victim, such as is available in California. I further believe that it does not allow the same amount of protection as is available in Texas- as individuals in Texas can still find remedy in subsection (b) for a misdemeanour, where the catfisher is not required to have engaged in any form of harmful conduct.

It has been shown that the various online impersonation/catfishing statutes enacted by the US States are not at all identical. However, they all contain exemplary examples of how effective regulations can deter catfishing. South Africa can learn from the US examples by possibly amending the current body of legislation, that is, the Cybercrimes Act.

V ANALYSIS AND RECOMMENDATIONS

The analysis of the USA's current legal framework regarding catfishing clearly shows that no State has found a "perfect" solution to deter catfishing. Highlighting the exemplary provisions from the USA has provided South Africa with a sufficiently well-established blueprint for the criminalisation of catfishing.

¹⁹¹ Ibid at 88.

¹⁹² Ibid.

¹⁹³ Ibid.

Firstly, the California Penal Code has enacted legislation allowing catfishing victims to claim both criminal and delictual remedies against the act of catfishing. This is the most fundamental inclusion needed in South Africa's legislation. Providing a "double" remedy allows for the effective deterrence and punishment of the crime of catfishing. It entitles the catfishing perpetrator to suffer either a fine or imprisonment, or both, through criminal remedies, and it further allows for damages, and/or an interdict, and/or an apology to be ordered through a delictual claim. The combination of these two punishments through criminal and delictual claims (which I will call a "double remedy") emphasises the harm that catfishing can cause to both the direct and indirect victims of catfishing and allows for proper deterrence and remedies to be made available to all victims in South Africa. South Africa can embody this double remedy through one piece of clear legislation, namely the Cybercrimes Act.

Secondly, under The Texas Penal Code, there are two types of criminal offences- mainly a "felony" and "misdemeanour". The felony constitutes a more serious offence created by catfishing under the Texas law system, while the misdemeanour is a less serious offence. Yet, both offences are punishable by the Texas legal system. I believe South Africa should adopt the scaffolded approach to catfishing- where the more serious offences (which would be the equivalent of a felony) of impersonation on a social media platform hold the repercussion of up to 10 years in prison, and or a fine of R100,000 (which is less than the R178 125,80 equivalent of \$10,000), while still upholding the deterrence aspect required. In terms of the "less serious" offences related to catfishing (which would be the equivalent of a misdemeanour), I submit that South Africa should continue using the "scaffolded" approach of Texas, but use the misdemeanour penalties provided for under the New York Penal Code. If South Africa were to follow the New York Penal Code's misdemeanour penalties in the scaffolded approach, the punishment would include either a fine of up to R10,000 or a one-year imprisonment. The method of scaffolding the different types of catfishing crimes will assist in deterring any form of catfishing crimes from occurring.

In terms of Oklahoma- we have learned that it is impractical to limit catfishing legislation to social media only; as technology is so rapidly evolving and adapting that any legislation with closed conditions, will very quickly become outdated. This means South Africa should adopt a "broader" section in the Cybercrimes Act that caters for all technologies, and not specifically to social media.

Lastly- unlike the other State codes that limit catfishing remedies to when there are the elements of intention to harm, intimidate, threaten or defraud by the catfisher, Arizona has broadened the requirements of their elements. Arizona's identity theft statute criminalises catfishing where the catfish had the intent to use another's identity without their consent for unlawful purposes. Arizona, therefore, only requires an unlawful purpose, which, according to the Cambridge dictionary (as there is no set definition under the Arizona code), encompasses any intention or performance that would be deemed to be unlawful under the law, which is much broader than the intention to harm, intimidate, threaten or defraud.¹⁹⁴ Arizona's code deems it a serious enough offence to use another individual's image or persona, regardless of whether the party suffered any economic loss or not. South Africa should adopt the broader approach to criminalising catfishing, as catfishing can encompass any unlawful conduct, including but not limited to fraud, impersonation, cyberstalking, intimidation, revenge pornography, child grooming, image rights infringements, defamation, privacy infringements and many more.

The above elements from the USA provide South Africa with an effective, and more inclusive manner to regulate catfishing. These elements include allowing for both a criminal and delictual claim. Secondly, creating a "scaffolded" approach within SA's legislation would include a more severe and less severe criminal offence depending on whether or not the catfishing took place on social media or not. Thirdly, the criminal conduct of a catfish should not be limited to the elements of intention to harm, intimidate, threaten or defraud a victim- but rather that stating any unlawful purpose (that does not have to amount to economic loss) is sufficient to be sanctioned under our legislation. And lastly, any catfishing legislation should not be limited to instances occurring on social media alone.

VI CONCLUSION

The Internet, especially its influence in the creation and boom of social media, has opened many doors for individuals to meet new people online- for both platonic, romantic and even entrepreneurial reasons. However, with this new boom of social media- one of the newest, greatest, and most complex issues it has created is the rise of cyber impersonation- colloquially known as catfishing. Although South Africa has remedies in place for certain aspects intrinsic to catfishing, we are in need of legislation that regulates this threat, especially considering that

¹⁹⁴“Unlawful Purpose” available at: <https://dictionary.cambridge.org/example/english/unlawful-purpose..>, accessed on 21 November 2023.

catfishing almost always includes two victims: the direct and indirect victim. South Africa's current remedies for catfishing include delictual remedies, the Cybercrimes Act, and *crimen iniuria*. Through the analysis of several US State statutes on the issue of catfishing has provided South Africa with a sufficiently comprehensive blueprint on how to criminalise catfishing.

I propose that South Africa would not need an entirely new piece of legislation dedicated to this, but rather that amendments to the Cybercrimes Act need to be made. By extracting these elements, it is clear there are three important elements that must be utilised in South Africa's catfishing legislation. Firstly, for both a criminal and delictual claim, the creation of a "scaffolded" approach to the legislation- which would include a more severe and less severe criminal offence depending on whether or not the catfishing took place on social media or not. Secondly, South Africa should not limit its legislation to only those affected by social media. Lastly, the criminal conduct of a catfish should not be limited to the elements of intention to harm, intimidate, threaten or defraud a victim- but rather that stating any unlawful purpose (that does not have to amount to economic loss) is sufficient to be sanctioned under our legislation. If these elements are included in South Africa's legal framework, through an amendment to the Cybercrimes Act, with the inclusion of a new section that solely focuses on the criminalisation of catfishing, it would create a solid base under which catfishing victims can find a legal remedy that is both attainable and will assist in retribution for their suffering. The recommendations made would further effectively deter criminals from even attempting to catfish victims, as there would be both criminal and delictual claims that they would be exposed to. Criminalising catfishing under South African legislation would place South Africa as one of the global forerunners that have criminalised cyber-impersonation.

VII BIBLIOGRAPHY

Books

- Broyles D. S. *Criminal Law in the USA* (2015).
- Burchell J. *Principles of Criminal Law* 5 ed (2016).
- Papadopoulos S. & Snail ke Mtuz S. (eds) *Cyberlaw @ SA: The law of the Internet in South Africa* 4th ed (2022) Van Schaick Publishers: Pretoria.
- Pollock J. M. *Criminal Law* 10th ed (2012).

Cases

- *Grütter v Lombard* 2007 4 SA 89 (SCA).
- *Isparta v Richter and Another* [2013] JOL 30782 (GNP).
- *Mogale and Others v Seima* 2008 (5) SA 637 (SCA) at paras [9] to [12] and [18].
- *Okundu v S* (CA&R117/16) [2016] ZAECGHC 131.
- *S v Brereton* 1971 (1) SA 489 (RA).
- *S v Sharp* 2002 (1) SACR 360 (CkHC).
- *Wells v Atoll Media (Pty) Ltd* [2010] 4 All SA 548 (WCC).

Internet Refrences

- “Unlawful Purpose” available at:
<https://dictionary.cambridge.org/example/english/unlawful-purpose>, accessed on 21 November 2023.
- Boyle E.”Protecting Your Instagram & Facebook From Hackers: Two-Factor Authentication Explained” *Phorest* June 21 2023, available at :
<https://www.phorest.com/blog/two-factor-authentication-explained/#:~:text=Simply%20go%20to%20your%20profile,enable%20it%20for%20your%20account>, accessed on 16 February 2024.
- Petrosyan “Worldwide digital population 2023” (22 May 2023), available at
<https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=Worldwide%20digital%20population%202023&text=As%20of%20April%202023%2C%20there,population%2C%20were%20social%20media%20users>, accessed on 13 June 2023.

Journal Articles

- Basdeo V. “Criminal and procedural legal challenges of identity theft in the cyber and information age” (2017) *South African Journal of Criminal Justice* 363.
- Martin B. N. “Mixing old and new wisdom for the protection of image based sexual abuse victims” (2022) *South African Journal of Criminal Justice* 307.
- Snail ka Mtuz S. “The Convergence of Legislation on Cybercrime and Data Protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013” *OBITER* (2022).

Journal Articles-USA

- Clanton K. “We are not who we pretend to be: ODR alternatives to online impersonation statutes” (2014) 16 *Cardozo Journal of Conflict Resolution* 323.
- Cohen M. “Angling for justice: Federal Law to reel in Catfishing” (2018-2019) 2 *Journal of Law and Technology at Texas* 51.
- Derzakarian A. “The dark side of social media romance: civil recourse for catfishing victims” (2017) 50 *Loyola of Los Angeles Law Review* 741.
- Santi A. “‘Catfishing’: A comparative analysis of the U.S. v. Canadian Catfishing Laws & their limitations’ (2019) 44 *Southern Illinois University Law Journal* 73.

Legislation

- Constitution of the Republic of South Africa, 1996.
- Cybercrimes Act 19 of 2020.
- Electronic Communications and Transactions Act 25 of 2002.

Legislation- USA

- Arizona Revised Statutes Title 13. Criminal Code § 13 (2008).
- California Penal Code § 528.5 (2022).
- Oklahoma Statutes Title 12 §1450 (2017).
- Texas Penal Code §33.07 (2011).

Magazine/ Newspaper Articles

- Geldenhuys K. “Scammed out of love” (June 2020) *Community-based Safety & Security Magazine* at 26.
- Schrieber S. “Unresolved cases: As crime increases, SAPS continues to lose detectives” *Times Live* 30 June 2023.

Unpublished Theses

- Ndyulo L. N. L. Ndyulo *Protecting the right to identity against catfishing* (unpublished LLM thesis, Rhodes University, 2021) at 1.