

**THE SUFFICIENCY OF PROTECTION IN LIGHT OF THE INCREASING
NUMBER OF CYBERCRIME AND CYBER HARASSMENT CASES.**

by

0411272M

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: 31 October 2022

DECLARATION

I declare that this submission is my own unaided work. It is submitted in partial fulfilment of the requirements of 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.



Signed: DANIEL WITZ

ACKNOWLEDGMENTS

I would like to express my heartfelt gratitude to my beautiful wife Isa for her unwavering support and understanding throughout my journey of pursuing a master's degree. Her constant encouragement, love, and patience have been the driving force behind this academic achievement. She has always been there for me, providing me with the necessary motivation and inspiration to keep going, even during the most challenging times. Her unwavering belief in me has been instrumental in helping me reach this milestone in my academic career. I am truly grateful for you, I love you.

To my amazing daughter Zoe, thank you for bringing us so much joy whilst I was pursuing a master's degree. As you enter this world and begin your journey through life, I want to take a moment to acknowledge the incredible gift you are to your mother and me. I cannot wait to see all the wonderful things you will accomplish in this life.

To my wife and daughter, this achievement is not just mine, but ours.

Abstract

This research examines how the South African Police Services, the National Prosecuting Authority, current and new legislation and Criminal Law address harassment in light of the increased threat and technological advancements of cyberbullying and cyber harassment. This research assignment will critically reflect on whether the Protection from Harassment Act, supported by recent additions to South African legislation, affords an applicant sufficient protection considering the increasing number of cybercrime and cyber harassment cases, and whether or not the reliance on the South African Police Services and South African Courts negates any protection that the legislation affords. In conclusion, this research report will make certain recommendations regarding how the complex issues of harassment can be addressed to focus on the protection of South Africa's Constitutional Values.

Keywords: Cyber harassment, virtual reality

LIST OF ACRONYMS

DVA	Domestic Violence Act 116 of 1998
DVA Bill	The Domestic Violence Amendment Bill
ECSP	Electronic Communications Service Provider
ECTA	Electronic Communications and Transactions Act 25 of 2002
EU	European Union
FPA	Films and Publications Act 65 of 1996
FPAA	Films and Publications Amendment Act 11 of 2019
GDPR	General Data Protection Regulation
ISP	Internet Service Provider
NPA	National Prosecuting Authority
PHA	Protection from Harassment Act 17 of 2011
SAPS	South African Police Services
SA	South Africa
USA	United States of America
VPN	Virtual Private Network
VR	Virtual Reality

TABLE OF CONTENTS

	Page
Title Page	1
Declaration	2
Acknowledgements	3
Abstract	4
List of Acronyms	5
I Introduction	7-9
II What are the Metaverse and Virtual Reality?	9-11
III What are Harassment and Cyber Harassment?	12-14
IV South Africa's Legal Framework	14-30
(a) Common Law position in South Africa	15
(b) The Constitution of the Republic of South Africa 1996 (The Constitution)	15-16
(c) The Protection from Harassment Act and Domestic Violence Act	17-18
(i) Process of Obtaining and Effecting Applications and Orders	18-19
(ii) Critique of the Applicant and Enforcement Process in relation to Cyber Harassment	19-23
(d) The Domestic Violence Amendment Bill (DVA Bill)	23-24
(e) Electronic Communications and Transactions Act 25 of 2002	24-25
(f) The Cybercrimes Act 19 of 2020	25-27
(g) Films and Publications Act 65 of 1996 and Films and Publications Amendment Act 11 of 2019 (FPAA)	28-31
V Case Law and Practicalities	31-38
VI Interaction between South African Police Service and Courts	38-40
VII International Trends	40-42

I INTRODUCTION

Web 2.0 began in 2004 and referred to the second stage of the development of the internet, characterised specifically by the change from static web pages to dynamic or user-generated content, and the advanced and accelerated growth of social media.¹ Since 2004, cyberbullying and cyber harassment have increased with the rise in use of social media platforms. There has been a sharp increase in cyber harassment, especially through social media platforms, which provide anonymity to the perpetrators.² During the global pandemic, governments instituted stay at home orders, which saw a significant increase in the average time users in the United States of America (USA) spent on social media in 2020. During 2020 a user, on average, would spend 65 minutes daily on social media platforms, compared to 54 minutes and 56 minutes in prior years.³ This would not be dissimilar from global statistics. The increase in social media activity would inevitably lead to increased use of such platforms for harassment. In February 2021, Digimune,, a digital identity, privacy and social media protection company, conducted a survey; This survey concluded that online child abuse, whether in the form of cyberbullying, cyberstalking and/or online shaming, is rising in South Africa. Approximately 51.5% of the children's parents who participated in the survey, stated that their children had been victims of cyber harassment. Statistics indicate that women and children are generally the most likely victims of such crimes.

¹ Web 2.0 is 'a term used to describe a generation of Web services and applications with an increasing emphasis on human collaboration'. accessed at <https://www.headland.co.uk/pages/gloassary> (last accessed on 14 March 2022).

² Smit, M.D. 'cyber bullying in South African and American schools: A legal comparative study' South African Journal of Education, Volume 35, Number 2, May 2015. Article No. 1076, 1 at 1.

³ Published by Statista Research Department, May 19, 2021, accessed at https://www.statista.com/topics/7863/social-media-use-during-coronavirus-covid-19-worldwide/#dossierSummary__chapter2, accessed on 8 January 2022.

Moreso, in South African schools, bullying is in the national spotlight after a Grade 10 Limpopo schoolgirl allegedly committed suicide after a video of her being assaulted by fellow pupils went viral.⁴ According to South African Police statistics released in 2020, nine murders and nineteen attempted murders recorded by police between April 2019 and March 2020 resulted from bullying in schools.⁵ These high statistics remain, despite the victims of cyber harassment, mainly school children, regularly reporting verbal threats, harassment, being made fun of, and rumour spreading.⁶ Oftentimes, cyber harassment may not entail direct harassment by the perpetrator, but rather the perpetrator inciting others to harass the victim (e.g. disclosing the victim's information to other people so that they may contact the victim). As of 2022, cyber harassment is not limited to viral videos or text messaging and has in fact spread to online virtual worlds. Harassment using electronic means appears to have a more menacing effect on children than traditional harassment, however, cyber harassment towards women is an ever present threat. One in ten women in the EU report having experienced cyber harassment since the age of fifteen. This includes receiving unwanted and/or offensive sexually explicit emails or SMS messages, or offensive and/or inappropriate advances on social networking sites.⁷

This essay aims to answer the following question: does South Africa's current legal framework cater for incidents of harassment in the world of Web3 and virtual reality, as the world's largest tech companies, namely Microsoft, Google, Apple et al storm headlong into creating the Metaverse? The reality is that traditional forms of

⁴ 1000 Women Trust 'Local NGO assists schools and parents with anti-bullying skills after Limpopo-tragedy' available at <https://www.news24.com/parent/learn/teacher-collection/local-ngo-assists-schools-and-parents-with-anti-bullying-skills-after-limpopo-tragedy-20210419> accessed on 14 March 2022.

⁵ South African Police Services, Crime Statistics, Crime Situation in the Republic of South Africa Twelve (12) Months (April to March 2021 - 2022).

⁶ Huang, Y and Chou, C 'An analysis of multiple among junior high school students in Japan' 2010 (26) *Computers in human behaviour* 1581 at 1585.

⁷ United Nations, Department of Economic and Social Affairs, Statistics Division (2020). Achieve gender equality and empower all women and girls.

harassment will always find their way into and form part of any advancement in technology, including the Metaverse, and there are very few mechanisms in place that allow users to easily report such misbehaviour in the real world. This will lead to even great obstacles in combatting cyber harassment in virtual worlds.

This paper deals with cybercrimes, and particularly cyber harassment, a crime that is committed through the use of technology, and impacts the emotional and mental health of its victims. This essay will first consider what the metaverse and virtual reality are and how it has created spaces that are no longer safe. Secondly, it discusses how such crimes infringe on the very dignity of an individual, who should be afforded protection as set out by the Constitution. In dealing with cyber harassment and the infringement of an individual's dignity, this research paper will offer a proposal that if the South African Police Services (SAPS), the National Prosecuting Authority (NPA), and complainants work together within the combined framework of the Cyber Act, the Domestic Violence Act 116 of 1998 (DVA), the Protection from Harassment Act 17 of 2011 (PHA) and the Films and Publications Act 65 of 1996 (FPA), an applicant can be afforded sufficient protection in light of the increasing number of cybercrime and cyber harassment cases.

II. WHAT ARE THE METAVERSE AND VIRTUAL REALITY?

On 1 December 2021, Facebook started to trade its shares under the Meta Platforms (Meta). Meta envisions a virtual world where digital avatars connect through work, travel, or entertainment using virtual reality (VR) headsets. Virtual reality is the computer-generated simulation of a three-dimensional image or environment that can be interacted with in a seemingly real or physical way through the use of a VR headset. Meta, the umbrella company formerly known as Facebook, has opened up access to its virtual-reality social media platform, Horizon Worlds.⁸ Horizon Worlds was designed

⁸ Horizon Worlds accessed at <https://www.oculus.com/facebook-horizon/> accessed on 8 January 2022.

to be fun and wholesome, allowing up to twenty avatars to get together at a time, where the avatars can explore limitless virtual worlds and build communities within their own virtual realities. The Metaverse is an essential future iteration of the internet and is an advancement from Web 2.0 to Web 3.0. Despite how technologically advanced the future of work, travel and entertainment may seem, on 3 February 2022, Meta's stock plunged more than 25% during its fourth-quarter financial results. Over and above the impact of Apple's new privacy measures and a drop in people using Facebook daily, it appears that the Metaverse is becoming more dystopian. In 2021, Facebook had already invested approximately US\$10 billion into the metaverse platform.⁹

Despite the social intentions of the platform, on 26 November 2021, a beta tester reported that a stranger had groped her on Horizon Worlds. There have been many instances where avatars are harassed, assaulted, bullied, and victims of hate speech in these virtual reality games. As of 2022, cyber harassment is not limited to viral videos or text messaging. Cyber harassment is 'an aggressive intentional act carried out by a group or individual using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend himself or herself.'¹⁰ It has been proven that the internet is a domain where people tend to lose their inhibitions to perpetrate acts of cyber harassment.¹¹ People who appear to lead ordinary lives offline, and have perfectly ordinary profiles online, can display a different personality in the digital realm – sometimes something more playful or open, but often something more sinister, giving in to the temptation of deviant behaviour induced by the drug of anonymity. This anonymity emboldens people to act with pseudonymity. Within this pseudonymity, problems begin to emerge in the virtual realm, resulting in real-world consequences. Perpetrators operate under the impression that there are no social repercussions, as they are untraceable. This impression stems from a false sense of security against both the

⁹ Mark Zuckerberg says Meta's metaverse project will lose 'significant' sums of money for up to 5 years accessed at <https://finance.yahoo.com/news/mark-zuckerberg-says-metas-metaverse-095455570.html>.

¹⁰ Pew Research Center, January 2021, 'The State of Online Harassment at 63.

¹¹ Anon, Cyberstalking: A Real Life Problem (Grafx-Specs, 1997), available at: http://www.safeteens101.org/cybstalker_prevention1.html (last accessed on 8 January 2022).

detection of identity and vigilance in law enforcement. The operation of Metaverse within Web 3.0, coupled with pseudonymity, allows people to act out their fantasies and express their innermost thoughts. In the real world, these thoughts and fantasies may be considered illegal, offensive, or objectionable.

A Pew Survey found that 33% of women under 35 had reported being sexually harassed online.¹² In December 2021, researchers for the Centre for Countering Digital Hate identified 100 potential violations of Meta's virtual reality policies, including sexual harassment and abuse.¹³ With approximately only 300,000 users worldwide, Horizon Worlds has quickly become a breeding ground for harmful content, according to a report published by the non-profit advocacy group SumOfUs.¹⁴

Meta's attempts at addressing these real-world issues that have bled into the Metaverse have been insufficient, as in May 2022, a researcher became a victim of sexual harassment. She had entered Metaverse to study users' behaviour on Horizon Worlds. Within an hour of her donning her Oculus virtual reality headset, she says she was raped in the virtual space.¹⁵ The researcher stated that her controller vibrated when male avatars touched her, resulting in a physical sensation being felt through the control, resulting in her online experience, immersed in the virtual world, feeling as if it was happening in the real world. It is increasingly so that harassment in the virtual world has real-world impacts and this research report will consider if the laws currently in place can effectively address these issues.

III. WHAT ARE HARASSMENT AND CYBER HARASSMENT?

¹² Pew Research Center, January 2021, 'The State of Online Harassment'.

¹³ Rachel Metz, 'Meta is giving avatars a four-foot buffer zone to cut back on VR harassment' 4 February 2022, available at <https://edition.cnn.com/2022/02/04/tech/meta-vr-avatar-safety-boundary/index.html> (last accessed on 14 March 2022)

¹⁴ Metaverse: another cesspool of toxic content accessed at https://www.sumofus.org/images/Metaverse_report_May_2022.pdf on 4 June 2022.

¹⁵ Researcher raped in Metaverse access at <https://www.businessinsider.co.za/researcher-claims-her-avatar-was-raped-on-metas-metaverse-platform-2022-5> on 4 June 2022.

Harassment is when an individual acts in a manner that causes another individual to fear harm¹⁶ and to negatively impact the victim's dignity. The harm suffered may be mental, psychological, physical, or economic.¹⁷ The PHA defines harassment as the act of:

'directly or indirectly engaging in conduct that the respondent knows or ought to know –

(a) Causes harm or inspires the reasonable belief that harm may be caused to the complainant or a related person by unreasonably –

(i) Following, watching, pursuing or accosting of the complainant or a related person, or loitering outside of or near the building or place where the complainant or a related person resides, works, carries on business, studies or happens to be;

(ii) Engaging in verbal, electronic or other communication aimed at the complainant or a related person, by any means, whether or not conversation ensues; or

(iii) Sending, delivering or causing the delivery of letters, telegrams, packages, facsimiles, electronic mail or other objects to the complainant or a related person or leaving them where they will be found by, given to, or brought to the attention, of the complainant or a related person; or

(iv) Amounts to sexual harassment of the complainant or economic harm;'

While the PHA broadly sets out what harassment is, the more traditional forms of harassment that we know of are: threats and intimidation; harassment or stalking; vilification and defamation; exclusion and identity theft. Despite technological advancement, these traditional forms of harassment have remained.. Harassment, with the use of technology has taken different forms and is now known as cyber harassment or cybercrime.

¹⁶ Section 1 of the Domestic Violence Act 116 of 1998.

¹⁷ South African Justice College, 2016, 'Harassment'.

The goal of a perpetrator engaging in cyber harassment is to negatively impact the victim's dignity. The harm suffered may be mental, psychological, physical, or even economic. With the increase in modern technology, mental, psychological, physical, or economic harm has taken on a much broader meaning. Technology has also allowed perpetrators greater access to individuals, and harassment is fast developing new forms faster than legislation can keep up. Technology has allowed perpetrators to harass globally without considering border restrictions. While the current legal framework can deal with the traditional forms of harassment sufficiently, Sulfab states that new laws are required to combat cybercrimes and cyber harassment, or current laws need to be amended.¹⁸

Cyber harassment, more frequently referred to as cyberbullying, is perpetrated using traditional forms of harassment via electronic means. Often, a perpetrator is able to remain nameless and faceless while continuing to harass an individual, causing the individual harm without the constraints of time and physical proximity to the individual. Such acts include 'repeated, harmful interactions which are deliberately offensive, humiliating, threatening and power assertive; that is performed through the use of electronic equipment, such as cell (mobile) phones or the internet by one or more individuals towards another.'¹⁹

Cyberstalking, a form of Cyber harassment, has become a concern for many jurisdictions, who have attempted to legislate on the issue. Often, cases of cyberstalking or harassment do go to court but end up being resolved through other pieces of law pertaining to computer misuse. Cyberstalking is more severe than traditional stalking. Traditional stalking causes anxiety and intense fear to a victim, who can combat it by having others around to protect him/her; with cyberstalking the victim additionally

¹⁸ Sulfab, M. 'challenges of cybercrime in South Africa' American University 2004 at 40.

¹⁹ Kift S, Campbell, M. and Butler, D. 'Cyber bullying in social networking sites and blogs: legal issues for young people and schools' 2009/2010 (20) *Journal of Law, Information and Science* 61 at 62.

has the anxiety of knowing that the stalker can access him/her at any time of day or night, wherever they may be, even if the stalker is not in close physical proximity to the victim. The victim ends up losing a sense of control in their life.

South Africa's current harassment laws aim to provide recourse for the traditional forms of harassment. However, it is my view that these laws do not sufficiently address the needs of the individual in the digital world. In an attempt to update current legislation, the newly enacted Cybercrimes Act 19 of 2020 (Cyber Act) not only creates new offences but also criminalises the disclosure of harmful data messages and including those that contain intimate images. These newly created offences within the Cyber Act now attract penalties. The Cyber Act aims to implement an integrated cybersecurity legislative framework to effectively deal with cybercrimes and address aspects pertaining to cybersecurity. In order to determine whether the Cyber Act has done enough to deter harassment, it is necessary to analyse South Africa's legal framework surrounding the prevention of cyber harassment.

IV SOUTH AFRICA'S LEGAL FRAMEWORK

One would need to understand what protections are afforded to victims of cyber harassment within the combined framework of the Cyber Act, the DVA, PHA, and the FPA. These three pieces of legislation will be analysed to determine whether there is sufficient protection. This section will first consider the common law position, the PHA and DVA, the Electronic Communications and Transactions Act 25 of 2002 (ECTA), the Cyber Act, and the FPAA.

a) Common Law Position in South Africa

The common law has provided us with many legal avenues that can still be used today, despite technological advancements. For example, the criminal law offences of *crimen*

injuria, assault (common), criminal defamation, and extortion are all offences that can be utilised in cases of cyber harassment. The offence of *crimen injuria*, which is the unlawful, intentional and serious violation of a person's dignity or privacy, accurately encapsulates the act of harassment.²⁰ The common law crime of criminal defamation includes the unlawful and intentional publication of a matter concerning an individual, thereby injuring that person's reputation.²¹ This includes defamatory remarks made on messaging services and/or social media platforms.

The common law remedies for *crimen injuria*²² are limited. A complainant can obtain an interdict prohibiting the respondent from messaging the applicant directly or indirectly and/or continuing to post defamatory remarks. Alternatively, a complainant can seek a claim of defamation. Unfortunately, access to such remedies is costly and lengthy.²³

b) The Constitution of the Republic of South Africa, 1996 (The Constitution)

With the start of a democratic South Africa, the Constitution became the supreme law. Section 2 of the Constitution states that all laws and conduct must be in line with the values of the Constitution.²⁴ The Constitution should prop up and strengthen current and new legislation to ensure the protection of Constitutionally enshrined rights in advancing technologies such as Web 3.0.

²⁰ Snyman, C.R. Criminal Law 5 Edition (2008) at 469.

²¹ Supra note 29 at 475.

²² an action that injures the dignity of another person.

²³ Section 30 of the Magistrate's Court Act 32 of 1944 and Rule 6 of the Uniform Rules of Court.

²⁴ The Constitution of the Republic of South Africa, 1996.

The Constitution has set out certain fundamental rights that apply to everyone. These are: the right to equality²⁵, privacy²⁶, dignity²⁷, freedom, and security²⁸ of the person, which may not be unreasonably and unjustifiably infringed. Constitutional rights are reliant on each other, so a violation of privacy could result in a violation of a corresponding right such as a person's dignity. In *Bernstein and others v Bester and Others NNO*,²⁹ the Constitutional Court emphasised that 'in South African law the right to privacy is recognised as an independent personality right which the courts have included within the concept of *dignitas*.³⁰ Dignity is a founding constitutional value and a constitutional right. Dignity gives human life value. It is attached to a person's self-worth and is central to the South African concept of ubuntu and uniting all other human rights into one.³¹ Human Dignity, as a constitutional value, lays the foundation for all of the rights enshrined in the Constitution and ensures that every person has the right to have rights.³²

This concept of dignity is explained succinctly in *S v Makwanyane* as:³³

'Generally, ubuntu translates as humaneness. In its most fundamental sense, it translates as personhood and morality....describing the significance of group solidarity on survival issues so central to the survival of communities. While it envelops the key values of group solidarity, compassion, respect, human dignity, conformity to basic norms and collective unity, in its fundamental sense it denotes humanity and morality. Its spirit emphasises respect for human dignity, marking a shift from confrontation to conciliation.'

²⁵ Ibid, Section 9.

²⁶ Ibid, Section 14.

²⁷ Ibid Section 10.

²⁸ Ibid, Section 12.

²⁹ *Bernstein and Others v Bester and Others NNO 1996 (2) SA 751 (CC).*

³⁰ *Ibid* at par 68.

³¹ Aharon Barak, *Human Dignity The Constitutional Value and the Constitutional Right*, pp. 103 – 113.

³² Christopher Enders, *Right to have Rights – The German Constitutional Concept of Human Dignity*, Volume 3, Issue 3 (2010).

³³ *S v Makwanyane and Another 1995 (2) SACR 1.*

The above extract from *S v Makwanyane* serves to amplify the importance of a person's dignity, which is why it is important that the legislature aims to protect a person from harassment that impairs a person's dignity.

c) The Protection from Harassment Act and Domestic Violence Act

This section will compare the PHA and the DVA rather than referring to them separately, as both the PHA and the DVA have similar implications and have unfortunately been equally poor when tested against matters involving cyber harassment.

The purpose of the DVA is to protect victims of domestic violence, and similarly, the PHA seeks to ensure the protection of an individual's fundamental rights. Both the DVA and the PHA ultimately ensure the protection of fundamental rights through a Court process, but the DVA and PHA apply to different types of relationships respectively. The DVA applies to parties in a domestic relationship.³⁴ Whereas the PHA offers broader protection, including situations where the suspect is unknown to the complainant.

Section 1 of the DVA clarifies and defines certain acts of domestic violence. One such form of abuse includes 'stalking', which is defined as 'repeatedly following, pursuing, or accosting the complainant', and emotional, verbal, and psychological abuse, which the DVA defines as:

*'a pattern of degrading or humiliating conduct towards a complainant, including –
(a) repeated insults, ridicule or name calling;*

³⁴ The complainant must be in a domestic relationship with the respondent such as a person to whom the complainant is or was married; the complainant lives or live within the same household; family members related by blood or legal relationship; complainant and respondent are or were engaged or in a romantic and/or sexual relationship.

(b) repeated threats to cause emotional pain; or
(c) the repeated exhibition of obsessive possessiveness or jealousy, which is such as to constitute a serious invasion of the complainant's privacy, liberty, integrity or security.'

Both the DVA and PHA cater for acts that do not require the physical presence of the perpetrator.³⁵ We must determine whether relying on the DVA and PHA provides sufficient protection for victims of cyber harassment. Cyber harassment is clearly an act of domestic violence in terms of the DVA. Unfortunately, the DVA is not adequately equipped to provide legal recourse to a complainant of cyber harassment. As such, complainants of cyber harassment can utilise the PHA to obtain a protection order.

i) Process of Obtaining and Effecting Applications and Orders

In terms of the DVA and PHA, when an applicant applies for an interim order, the court must grant an interim protection order if it is satisfied that harm will continue to be suffered.³⁶ The complainant brings an application for a protection order *ex parte* by way of an affidavit, without notice being given to the respondent. The PHA also makes provision for the application to be brought on behalf of the complainant by another person who has a material interest in the well-being of the complainant.³⁷ In the matter of *S v Trainor*³⁸, the court held that '[e]vidence, of course, must be evaluated against the onus of any particular issue or in respect of the case in its entirety.' The onus in harassment cases conducted electronically or otherwise is on the complainant to show

³⁵ Section 1, Domestic Violence Act 116 of 1998 and Section 1, Protection of Harassment Act 17 of 2011.

³⁶ Section 3, Protection of Harassment Act 17 of 2011.

³⁷ section 2(3), Protection from Harassment Act 17 of 2011.

³⁸ *S v Trainor 2003 (1) SACR 35 (SCA)*.

that they are entitled to protection against the perpetrator as the perpetrator's conduct constitutes harassment in terms of the DVA or any other applicable legislation.³⁹

Once granted, an interim protection order is formally served on the respondent via the SAPS. The respondent is called upon to show good cause as to why a final order should not be granted.⁴⁰ This process gives rise to a multitude of logistical problems. What occurs when the respondent is unknown to the applicant or is hiding behind a pseudonym? To who and how would the SAPS be able to formally serve the order? While these issues are of great concern, one must also not forget that the SAPS has limited resources to investigate such matters. Therefore, additional resources and training would need to be provided to the SAPS to deal with these cases.

When the clerk of the Court receives the return of service confirming that the interim order was served on the respondent, then the Court will issue a warrant of arrest for the respondent and provide the complainant with a copy.⁴¹ Any interim or final order granted needs to be drafted to specifically include indirect methods of harassment, including but not limited to the use of pseudonyms if the applicant can prove that the harasser is the same person. This is currently not happening, as our Courts are simply referring broadly to indirect methods of harassment.

ii) Critique of the Applicant and Enforcement Process in relation to Cyber Harassment

On considering the practicalities of the processes explained above, when dealing with cases of cyber harassment, the PHA, unlike the DVA, allows the court to issue an order requesting an electronic communications service provider (ECSP) to furnish particulars

³⁹ Ibid at para 9.

⁴⁰ s 3(3) and (6) Protection from Harassment Act 17 of 2011 and Section 5(7) of the Domestic Violence Act 116 of 1998.

⁴¹ Section 3(7), Protection of Harassment Act 17 of 2011 and Section 4(3) of the Domestic Violence Act 116 of 1998.

to the court to assist in identifying an unknown perpetrator.⁴² The PHA also allows the court to issue a direction, instructing the ECSP to provide the court with the identity of the harasser. More importantly, the PHA criminalises cyberstalking. These additions to the PHA are welcomed, but are not enough to keep up with the advancements in technology, and do not effectively protect a person's fundamental rights. The PHA and DVA can be made more effective if the legislation allows a person to compel an ECSP and social media companies, either through a Court order, or through further regulations to be able to enforce such orders.

Another flaw in the PHA is that it does not factor modern forms of cyber harassment into its regulations, where a perpetrator may use a Virtual Private Network (VPN)⁴³ or fake email addresses etc., to carry out such acts. In such instances, the Internet Service Provider (ISP) cannot provide the court with the harasser's identity or location. A VPN masks the user's internet protocol address,⁴⁴ and VPN vendors do not keep a record of online activities. Therefore, even if law enforcement officials request such information from a VPN provider, the provider will be unable to comply since they do not have this information. Many countries have attempted to place restrictions on the use of a VPN, primarily due to the increase in cybercrime.⁴⁵ The use of VPN is currently legal in South Africa (SA). The author believes it unwise to place restrictions on the use of VPNs, as they provide many benefits, such as their built-in protective measures which protect individuals' personal information. Thus, VPN's safeguarding abilities align with SA's latest regulations in protecting personal information. The downside is that by using a VPN the applicant could end up with a 'hollow' court order, as it is impossible to identify the perpetrator.

⁴² Section 4, Protection of Harassment Act 17 of 2011.

⁴³ A virtual private network is an arrangement whereby a secure, apparently private network is achieved using encryption over a public network, typically the internet.

⁴⁴ An internet protocol address is a unique string of characters that identifies each computer using the Internet Protocol to communicate over a network.

⁴⁵ Court Uncourt Legal Magazine issue 10, Legalities of Using Virtual Private Network.

Any DVA application, must first and foremost show that a domestic relationship exists with the respondent.⁴⁶ Secondly, the complainant's evidence, initially adduced by way of affidavit, will have to, on a balance of probabilities, show that an act of domestic violence, as defined by the DVA, has been or is being committed. In other words, once the applicant has established a domestic relationship, the applicant must show that domestic violence occurred.⁴⁷ Harassment, regardless of whether in the DVA or the PHA, is difficult to prove in any legal forum, as it is a subjective experience. In *SATAWU obo Dlamini v Transnet Freight Rail, a Division of Transnet Ltd and Another*⁴⁸ it was held that the Constitution requires that the primary focus when determining harassment be on the effect it has on the complainant. The court further held 'that the proper test for assessing if the conduct was indeed harassment is by reference to the '*reasonable victim*' instead of the usually applied objective test of the reasonable person.'⁴⁹

This author believes that the DVA provides victims protection against cyber harassment but fails to empower victims of cyber harassment with practical mechanisms. In support of the author's view, the applicant having to provide *prima facie* evidence is an arduous and expensive task. The nature of cyber harassment lends itself to evidence-gathering processes that usually require the intervention of experts in the field. Secondly, if a domestic relationship does not exist between the applicant and the respondent, the applicant is not afforded protection under the DVA. As a result of this void, the PHA was enacted to remedy the DVA's shortcomings.

⁴⁶ Section 1 of the Domestic Violence Act 116 of 1998. A relationship between the complainant and respondent, including being married or having been married; co-habitation or having co-habited; being parents of a child or sharing parental responsibilities for that child; having been in a relationship; and sharing or having recently shared the same residence.

⁴⁷ Section 5(2)(a) and 6(4) of the Domestic Violence Act 116 of 1998.

⁴⁸ *SATAWU obo Dlamini v Transnet Freight Rail, a Division of Transnet Ltd and Another* [2009] JOL 24429 (Tokiso).

⁴⁹ *Ibid* at 51.

The PHA broadly defines 'harassment' and 'harm' but does not restrict the definition to physical or verbal abuse, nor does the PHA require a relationship to exist between the parties. A complainant can bring a claim against someone unknown to them.⁵⁰ The PHA does require that a perpetrator's conduct causes the complainant harm. Harm includes: watching, accosting, or loitering near the building where the complainant resides, studies, or works; engaging in verbal, electronic or other communication aimed at the complainant; the sending or delivery of written communications via, for example, letters, packages, or email; and finally, behaviour amounting to sexual harassment.⁵¹

It is the author's opinion that the PHA and DVA, on their own, fail to adequately safeguard respondents from vexatious applications, as an applicant can bring multiple applications without fearing that adverse orders will be made against them. Furthermore, the court proceedings are generally drawn out for months, with parties incurring unnecessary legal expenses. A respondent would have a right of anticipation, but this does not cure the flaws in the PHA and DVA.⁵²

The author believes that more streamlined requirements are needed, , such as providing actual documentary evidence, like a WhatsApp chat history, on making an application in terms of either PHA or DVA. However, in instances where there is a real danger and an applicant requires an order almost immediately, resources such as legal aid should be deployed at the Courts to assist applicants to comply with stricter requirements - currently applicants are simply handed a form to fill in with no guidance given. The complainant must comply with these requirements before the court will hear the *ex parte* application. If the respondent can present contradicting evidence, the courts should not hesitate to make costs orders against vexatious litigants.

⁵⁰ Section 1, Protection of Harassment Act 17 of 2011.

⁵¹ Section 1(1), Protection of Harassment Act 17 of 2011.

⁵² s 3(5) Protection from Harassment Act 17 of 2011 and Section 3(5) of the Domestic Violence Act 116 of 1998.

The courts should also invoke the processes of the CPA, allowing for vexatious complainants to be prosecuted where it has been proven that the complainant made materially false statements in their affidavits. The Domestic Violence Amendment Bill has recently been introduced to remedy the shortfalls of the DVA.

d) The Domestic Violence Amendment Bill (DVA Bill)

The proposed amendments in the DVA Bill include revised and new definitions of domestic violence. The revised definition of domestic violence includes economic abuse; emotional, verbal, or psychological abuse; intimidation, and physical abuse. Most important, for the purposes of this essay, is the revised definition of harassment, which now includes:

- 'Specified forms of disclosure of, or unauthorised access to electronic communications;
- Monitoring or tracking of a complainant's movements, activities, or interpersonal associations;
- Unreasonable interference with a complainant's exclusive use of property'.

Notably, the DVA Bill has deleted the stand-alone definition of 'stalking'⁵³ and incorporated it into the revised definition of 'harassment'. Further proposed amendments include:

*'Coercive Behaviour' which means 'to compel or force a complainant to abstain from doing anything that they have a lawful right to do, or to do anything that they have a lawful right to abstain from doing.'*⁵⁴

⁵³ The Domestic Violence Act 116 of 1998, Section 1(xxiii). defines stalking as 'repeatedly following, pursuing or accosting the complainant'.

⁵⁴ Section 1 of the Domestic Violence Amendment Act, 2021.

'Controlling Behaviour' meaning 'behaviour towards a complainant that has the effect of making the complainant dependent on, or subservient to, the respondent' and includes isolating a victim from sources of support; exploiting their resources or capacities for personal gain; depriving them of the means needed for independence, resistance or escape; or regulating their everyday behaviour'.⁵⁵

The DVA Bill has also incorporated new terms of abuse, which include the abuse of the elderly. The abuse of elderly females, 60 years or older, and males, 65 years or older, now includes any conduct or lack of appropriate action occurring within a domestic relationship where there is an expectation of trust, which causes or is likely to cause harm or distress to an older person.⁵⁶ Secondly, exposing a child to domestic violence.⁵⁷ Thirdly, the DVA Bill has included the related person abuse, which involves committing, or threatening to commit, acts of physical violence or damage to the property of any member of the family or household of a complainant.⁵⁸ The DVA Bill extended the pre-existing definition of 'sexual abuse' to include sexual harassment.⁵⁹ Lastly, the DVA Bill has included spiritual abuse, which prohibits the advocating of hatred against the complainant because of their religious or spiritual beliefs and constitutes incitement to cause harm to the complainant.⁶⁰

e) Electronic Communications and Transactions Act 25 of 2002

Prior to the enactment of the Cyber Act, the ECTA protected individuals against cyber-related offences. Chapter 13 deals mainly with cybercrimes, including the abuse of electronic communications or information systems to degrade, humiliate or harass another person.⁶¹ This includes instances where an individual hacks into another

⁵⁵ Ibid note 59.

⁵⁶ Ibid note 59.

⁵⁷ Ibid note 59.

⁵⁸ Ibid note 59.

⁵⁹ Ibid note 59.

⁶⁰ Ibid note 59 at 8.

⁶¹ Chapter 13 of the Electronic Communications and Transactions Act 25 of 2002.

person's electronic systems in order to intimidate, harass or threaten the person.⁶² The ECTA is seldomly used in matters involving cyber harassment, and victims usually resorted to either the PHA or DVA in matters of cyber harassment. The lack of protection is because the ECTA's primary purpose is to regulate economic transactions and not necessarily cybercrimes.

f) The Cybercrimes Act 19 of 2020

The Cyber Act came into effect on 1 December 2021. The Cyber Act is a much-needed addition to South Africa's legal framework, as it aims to offer protection of South Africans' personal data, and personal devices, as well as add protection to the utilisation of the networks and infrastructure of the internet. In addition, the Cyber Act has created offences that have a bearing on cybercrime. The offences include, but are not limited to, the criminalisation of the disclosure of harmful data messages, providing for interim protection orders, regulating powers to investigate cybercrimes, and to provide that South Africa may enter into agreements with foreign States to promote measures aimed at the detection, prevention, mitigation and investigation of cybercrimes. Despite previous Acts that tried to regulate cybercrimes, there was a need to deal with the competing, unbalanced interests of internet users and the interests of victims. The Cyber Act aims to develop modernised legal frameworks to address harassment. As such, the Cyber Act has criminalised specific aspects of harassment that occur through electronic means to threaten a person.⁶³

Despite the sections dealing with the issuing of protection orders not being operational,⁶⁴ similarly to the PHA the Cyber Act allows a complainant to apply to a Magistrates court for a protection order pending an investigation of a crime committed

⁶² Supra note 38, Section 86 to 88.

⁶³ Section 15, Cybercrimes Act 19 of 2020.

⁶⁴ Part VI of Chapter 2, Cybercrimes Act 19 of 2020.

under the Act.⁶⁵ A court may also, under the Cyber Act, direct a service provider to furnish the particulars of the perpetrator. The PHA incentivises service providers' cooperation by providing that the Minister of Justice, where relevant, may compensate the service provider that provides information to law enforcement.⁶⁶ The Cyber Act creates twenty new cybercrime offences with the intention to provide legal authority on how to deal with cybercrimes. These crimes include: the unlawful access to a computer or device such as a USB drive or an external hard drive; the illegal interception of data; the unlawful acquisition, possession, receipt or use of a password and online forgery, fraud and extortion. The Cyber Act has made cyber harassment a punishable offence.

A shortcoming of the DVA and PHA, both in respect of cyber harassment and harassment in general, is that no mechanisms are provided as to how harassment offences should be investigated; this is left up to the SAPS, who have limited to no training in cyber related crimes and still work with hard copy dockets. The DVA and PHA focus more on the victims, and forget to guide the officials assigned to secure the rights of the victims.⁶⁷ Victims of cybercrimes are still required to report at local police stations, most of which local do not have the personnel or equipment to deal with cybercrimes adequately. Usually, only once a case docket has been opened will the matter be referred to the SAPS Cyber Crime and Deep Web Investigation Unit. Unfortunately, most governmental departments are understaffed and underfunded in South Africa. Unlike the DVA and the PHA, The Cyber Act now creates mechanisms for conducting such investigations, including searching and gaining access to, or seizing items in relation to cybercrimes.

⁶⁵ Section 20, Cybercrimes Act 19 of 2020.

⁶⁶ Section 4(8) Protection of Harassment Act 17 of 2011.

⁶⁷ Mogale S et al : *Violence Against Women in South Africa: policy Position and Recommendations*, 2012.

Certain sections of the Cyber Act are yet to be made operational and inoperative legislation is not good enough since it cannot prevent perpetrators from participating in future unlawful conduct. Most notably, section 16 dealing with revenge porn.⁶⁸ The prohibition on revenge porn in section 16 of the Cyber Act deals with the harmful disclosure of pornography where an individual discloses intimate images and/or videos of another person, most commonly on social media and messaging platforms, without that person's consent, with the intention of causing harm, 'including mental, psychological, physical, social or economic harm'. Until this section of the Cyber Act becomes operational, revenge porn cases are dealt with under the law of defamation, breach of an individual's right to dignity,⁶⁹ right to privacy,⁷⁰ and a breach of contract in terms of which a victim may have consented to the photos and videos being filmed. An argument could also be made in respect of the Copyright Act 98 of 1978 (Copyright Act), which is unique in that copyright is subject to protection by criminal law. The criminal provisions of the Copyright Act are embodied in section 27.⁷¹ An individual can look to hold a website liable for republishing their copyrighted photos should a website not comply with a takedown request.

g) Films and Publications Act 65 of 1996 and Films and Publications Amendment Act 11 of 2019 (FPAA)

The FPAA aims to amend current legislation to include instances of cyber harassment. The FPAA aligns the definition of child pornography to the more broad definition set

⁶⁸ Section 11B, 11C, 11D and Section 56A(3)(c) – (e) of the Criminal Law (Sexual Offences and Related matter amendment Act).

⁶⁹ Ibid note 1 at section 10.

⁷⁰ Ibid note 1 at section 14.

⁷¹ Copyright Act 98 of 1978, as amended at Section 27(6) 'A person convicted of an offence under this section shall be liable - (a) in the case of a first conviction, to a fine not exceeding five thousand rand or to imprisonment for a period not exceeding three years or to both such fine and such imprisonment, for each article to which the offence relates; (b) in any other case, to a fine not exceeding ten thousand rand or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment, for each article to which the offence relates.'

out by the Constitutional Court judgment in the case of *De Reuck v DPP*.⁷² In this case, the Court held that section 27(1) constitutes a reasonable and justifiable limitation on the section 16 right to freedom of expression. This is an important juxtaposition because although the writer contends that the fundamental rights in the Constitution should be protected, current and new legislation should allow for reasonable and justifiable limitations of fundamental rights. Ultimately, this limitation would be to protect other fundamental rights. In *De Reuck v DPP*, the limitation of freedom of expression protected the dignity of children, by stamping out the market for photographs made by abusing children.

The definition of sexual conduct is becoming more complicated, especially in the online world. It, therefore, requires amending. The definition of sexual conduct now aligns with the definition contained in the Criminal Law (Sexual Offences and related matters) Amendment Act 32 of 2007. Unlike the PHA and DVA, the FPAA, enacted prior to the Cyber Act, attempted to develop protections against online forms of harassment, including the prohibition of the distribution through any medium, including the internet and social media, of a private sexual photograph or film if the disclosure is made without the consent of the individual who appear in the photograph or film and with the intention of causing that individual harm. The FPAA provides a fine or imprisonment of an individual who intentionally distributes private sexual photographs and films in any medium, including online and social platforms, without the prior consent of the individual in the said sexual photograph or film, with the intention to cause the individual harm.⁷³

⁷² *De Reuck v DPP 2004 (1) SA 406 CC*. ‘child pornography’ is defined to include any image, however created, or any description of a person, real or simulated, who is or who is depicted, made to appear, look like, represented or described as being, under the age of 18 years— (a) engaged in sexual conduct; (b) participating in, or assisting another person to participate in, sexual conduct; or (c) showing or describing the body, or parts of the body, of such a person in a manner or in circumstances which, within context, amounts to sexual exploitation, or in such a manner that it is capable of being used for the purposes of sexual exploitation.

⁷³ Section 24E Films and Publication Amendment Act 11 of 2019.

An important development in preventing cyber harassment is in the Sexual Offences Amendment Act 32 of 2007 (Amendment Act).⁷⁴ It provides that '*harmful*' means causing emotional or psychological distress to a person, whether through a film, game, or publication, online or offline.⁷⁵ The definition of 'harm' corresponds with the harmful effects of cyber harassment. Most importantly, no person may create, produce or distribute in any medium, including the internet and social media, any films or photographs depicting sexual violence and violence against children. The creation, production, or distribution in any medium, which includes online and social media platforms depicting sexual violence and violence against children, is unlawful.⁷⁶

Until the Prevention and Combating of Hate Crimes and Hate Speech Bill is enacted, the FPA governs the prohibition against any person from distributing through any medium including the internet and social media, any film, game, or publication which amounts to propaganda for war, incites imminent violence, or advocates hate speech.⁷⁷ This is further prohibited in terms of the Constitution of the Republic of South Africa, Act 108 of 1996 (Constitution).⁷⁸

The PHA and the DVA allow an applicant to lodge an application with the clerk of a Magistrates Court to issue a protection order.⁷⁹ Unfortunately, the implementation of the PHA and DVA has been extremely poor in respect of cyber harassment⁸⁰, and the criminal penalties imposed by the Cyber Act do not give any further protection, which is why our Courts need to find harmonisation between all the legislation dealing with harassment. Although the Cyber Act imposes direct criminal consequences for

⁷⁴ Section 1(b), Films and Publication Amendment Act 11 of 2019.

⁷⁵ Ibid Section 1(j).

⁷⁶ Ibid Section 18G.

⁷⁷ Ibid Section 1(j).

⁷⁸ Section 16(2) of the Constitution of the Republic of South Africa, 108 of 1996.

⁷⁹ Section 2, Protection of Harassment Act 17 of 2011 and Section 4(3) of the Domestic Violence Act 116 of 1998.

⁸⁰ Are your hands tied when it comes to cyber harassment? Available at <https://www.derebus.org.za/are-your-hands-tied-when-it-comes-to-cyber-harassment/>.

actions such as sending threatening messages to someone with violence, or sending inappropriate sexual images of a person, the consequences only occur after the harassment has occurred or continues to occur. The current legal framework is a hybrid of legislation and the common law; however, it is reliant on dealing with matters on a case-by-case basis regardless of the ever-evolving nature of cyber harassment. The SAPS are also dragging behind in both their practical training and resources on how to implement Court Orders prohibiting the continuation of cyber harassment, nor do they have the inclination or resources to punish the offenders.⁸¹

The Cyber Act, although a step in the right direction as a piece of specialised legislation aligning South Africa with international norms, is still reliant on the SAPS and the NPA to investigate and prosecute within the mechanisms afforded by the Cyber Act.

V CASE LAW AND PRACTICALITIES

In reporting any act of cyber harassment, the complainant must set out that there was pain and fear or that there was a reasonable apprehension of harm. This is in order to show that an individual suffering from such acts should be afforded the protection provided for in anti-harassment legislation.⁸² CB Prest SC, submits that a reasonable apprehension of harm is one which a reasonable person might entertain on being faced with the facts, which the court finds to exist on a balance of probabilities. ‘*The test for apprehension is an objective one. The applicant must therefore show objectively that his apprehensions are well grounded. Mere assertions of his fears are insufficient. The*

⁸¹ The Portfolio Committee on Police in May 2022 raised concern about complaints lodged against members of the SAPS for the period between 1 April to 30 September 2021 include 15 cases of failure to open a case, two cases of failure to file a protection order, and two cases of failure to render satisfactory service to the victim. Further concern was raised about cases that were reported in the period between 1 October 2020 - 31 March 2021 that are still to be finalised by the SAPS.

⁸² Walker, C.M. ‘*Twenty-First century cyber bullying defined: An analysis of intent, repetition, and emotional response.*’

*facts grounding his apprehension must be set out in the application to enable the court to judge for itself whether the fears are indeed well grounded.*⁸³

Unfortunately, our Courts are more inclined towards evidence of repetitive behaviour constituting cyber harassment, rather than single incidents. The DVA and PHA each essentially, require that the conduct complained of should be repetitive. The writer is of the view that there are down sides to the requirement of seeking incidents of a repetitive nature. The very purpose of the DVA, as set out in its preamble, states that ‘*domestic violence is a serious social evil.*’ In instances where victims of domestic violence are among the most vulnerable members of society, just one incident of domestic violence should be considered enough to create fear, hence allowing a victim to access the remedies available in the DVA or the PHA. As an example, sexual harassment in the context of labour law need only occur once to be considered serious enough to afford protection to the victim; it need not be repetitive.⁸⁴ With the growing rates of gender-based violence in South Africa, is the law sufficient in saying that it must be repetitive, or could it be a once-off incident, which, if a Court considers it sufficient, could avoid an even worse fate being suffered by the victim?

As with all general rules in law, there are exceptions. In the case of *Mnyandu v Padayachi*,⁸⁵ the Court held that the singular conduct was of such an overwhelmingly oppressive nature that it held the same consequences as repetitive behaviour, as in the case of a single protracted incident when the victim is physically stalked.⁸⁶ The court held further that the conduct, when viewed reasonably, must not merely be unattractive or even unreasonable, but rather it needs to be oppressive and unacceptable, with the harm being serious enough to cause fear, alarm, or distress. In

⁸³ CB Prest SC The Law and Practice of Interdicts (Cape Town: Juta 1996) at p45.

⁸⁴ Violence and harassment in the world of work: A guide on Convention No. 190 and Recommendation No. 206 International Labour Office – Geneva: ILO, 2021.

⁸⁵ *Mnyandu v Padayachi 2017 (1) SA 151 (KZP).*

⁸⁶ Ibid note 87 at para 68.

Silberberg v Silberberg and Another,⁸⁷ Cloete AJ highlighted the various provisions of the DVA, emphasising that there needs to be a pattern of past conduct or repetition to conclude that there is a reasonable apprehension of such conduct occurring in the future.⁸⁸ In *Gouws v De Lange and Another*,⁸⁹ Revelas J found that the conduct complained of had been repeated at various stages over a period of approximately eighteen months, and that this demonstrated that the respondent was unable to restrain himself. It also found that the conduct went far beyond freedom of expression and opinion and was intended to inflict harm.⁹⁰

Most significant cases appearing before South African Courts are seeking not to punish offenders, but rather to protect against the potential of future harm. This is exhibited in *S v Baloyi* (Minister of Justice and Another Intervening)⁹¹ where the Court held:

*'The principal objective of granting an interdict is not to solve domestic problems or impose punishments, but to provide a breathing space to enable solutions to be found; not to punish past misdeeds, but to prevent future misconduct.'*⁹²

The question must be asked, is there any deterrence against future conduct without the risk of punishment? Further, is the past conduct complained of able to lead the trier of the facts and evidence to the conclusion that a reasonable apprehension exists on a balance of probabilities? Unfortunately, without legislative guidance the mechanisms necessary to find a balance between being over-cautious and being

⁸⁷ *Silberberg v Silberberg, Silberberg v Silberberg and Another* (A 603/2007, 4581/2008) [2013] ZAWCHC 5 (29 January 2013).

⁸⁸ *Ibid* note 89.

⁸⁹ *Gouws v De Lange and Another* (2842/14, 3449/14, 3450/14) [2014] ZAECPHC 89.

⁹⁰ *Ibid* note 91.

⁹¹ *S v Baloyi and Others* 2000 (2) SA 425 (CC).

⁹² *Ibid* note 93 at para 17.

dismissive are found wanting. In *Van Berg v Coopers and Lybrand Trust (Pty) Ltd and Others*⁹³, the Court found that 'resolving the tensions between every human being's constitutionally enshrined rights both to freedom of expression and to *dignitas* is all about balance.'⁹⁴ Further, how do our Courts prevent applicants from approaching the Courts with ulterior motives? Often our Courts would apply the *de minimis* principle in assessing the conduct, as was held in *S v Visagie*⁹⁵:

*'It seems to me that, wherever the defence of de minimis non curat lex is raised, the court has to consider all the circumstances under which the blow which is said to be trivial was delivered. In some circumstances, a blow may be considered so trivial as to justify the court ignoring it altogether, in different circumstances, a similar blow might be a relatively serious assault; for example, slaps delivered by fishwives to each other during a drunken brawl might well be ignored on the principle of de minimis non curat lex whereas an unprovoked slap delivered to the face of a lady, say at a garden party, could not be similarly ignored.'*⁹⁶

But this does not mean that all minor conduct should be tolerated or discomfort endured; rather, only in certain instances should conduct be recognised for what it is. More specifically, in relation to instances of cyber harassment, in the matter of *H, WS v W*, N⁹⁷ an applicant applied for an order to interdict a respondent from posting any information on Facebook about the applicant.⁹⁸ This case together with the matter of *RKM v RLB*, where an application was brought to request the removal of a post from

⁹³ *Van der Berg v Coopers & Lybrand Trust (Pty) Ltd and Others* [2001] 1 All SA 425 (A).

⁹⁴ Ibid note 95.

⁹⁵ *S v Visagie* 2009 (2) SACR 70 (W), quoting *R v Maguire* 1969 (4) SA 191 (RA).

⁹⁶ Ibid note 97 at 193.

⁹⁷ *H v W* [2013] 2 All SA 218 (GSJ) (30 January 2013).

⁹⁸ Ibid note 99 at par 34.

Facebook, dealt more with the privacy issues and control aspects of Facebook profiles.⁹⁹ Willis J, in *H v W*¹⁰⁰ stated:

‘Those who make postings about others on social media would be well advised to remove such postings immediately upon the request of an offended party. It will seldom be worth contesting one's obligation to do so.’

On 28 July 2020, the matter of *SR v Facebook Inc*¹⁰¹ was heard before Spilg J. In this case, a teenager was anonymously harassed with threatening messages of gang rape and murder, which required her to navigate an international administrative nightmare to compel Facebook Inc to disclose the identity of the holder/s of several Instagram accounts used to make the threats.¹⁰² ‘The use of fake online profiles and the anonymity of the internet can create difficulties for victims and the police in tracking perpetrators of online harassment, further exacerbated if the perpetrator is unknown to the victim.’¹⁰³ There is always a digital trace, however as set out previously, if a public network (or VPN) is used to facilitate abusive behaviour online, it can be impossible to track the perpetrator. In *SR v Facebook Inc*, when the abuse comes from outside the jurisdictional territory (or the service provider through which it was conducted is outside), then law enforcement has to attempt to get other jurisdictions and service providers to cooperate. Service providers like Facebook and Twitter have been reluctant in the past to release information to protect people's privacy in line with the General Data Protection Regulation (GDPR)¹⁰⁴.

⁹⁹ *RKM v RLB case no: 10175/2013* at par 12.

¹⁰⁰ Ibid note 99 at par 43.

¹⁰¹ *SR VS Facebook Inc 2020/1482728* July 2020.

¹⁰² Ibid note 103.

¹⁰³ ‘Are Your Hands Tied When It Comes to Cyber Harassment?’ De Rebus, 31 Aug. 2018 available at www.derebus.org.za/are-your-hands-tied-when-it-comes-to-cyber-harassment/. Accessed 29 Oct. 2022.

¹⁰⁴ EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

Often when social media networks cooperate, they merely deactivate the ‘fake account’, but this is not an obstacle for the perpetrator, who creates a new account to harass his/her victim. When issues like these are reported to the local police, they inform the victim that there is little they can do because of the number of fake profiles and the use of proxy servers¹⁰⁵. ‘Currently, under European Law, social media networks are protected under the e-Commerce Directive (2000/31/EC), regarded as hosts rather than publishers’. There is also the issue of compliance with GDPR.¹⁰⁶ This hinders the process of finding the actual perpetrators because they can hide behind VPNs and random IP addresses. Unfortunately, the SAPS are limited in their capabilities to breach the many walls protecting the perpetrators.

In *SR v Facebook Inc*, the Applicant requested that the identity of the holder/s of the Instagram accounts be disclosed due to a suspicion that the threats may have been made by someone who attends school with the teenager. However, the difficulty arises with the global reach of social media platforms. The application was brought against an entity that is incorporated in the USA. Instagram only holds basic subscriber information, which is key to identifying the perpetrator. The applicant faced numerous obstacles, not only jurisdictionally, but the Court suggested that she lodge a criminal complaint with SAPS. Unfortunately, the SAPS are not equipped to investigate such a matter as their first port of call would be to issue a section 205 subpoena¹⁰⁷ for Facebook Inc to hand over the information, which would take a minimum of six months. According to Statistics South Africa, only 62,7% of individuals who experienced crimes in South Africa reported some or all incidences to the SAPS. This could be an indication of the public's faith in the SAPS of solving a crime for various crime categories.¹⁰⁸

¹⁰⁵ A. Mmabthao, *South African Police Service capacity to respond to cybercrime: challenges and potentials*, Journal of Southwest Jiaotong University.

¹⁰⁶ This will be discussed in paragraph VI below.

¹⁰⁷ Section 205 of the Criminal Procedure Act 51 of 1977.

¹⁰⁸ Governance, Public Safety and Justice Survey (GPSJS) Victims of Crime 2020/21, Risenga Maluleke Statistician-General.

This case is a clear example of an applicant with sufficient economic resources to confront all the hurdles, yet still facing a long, drawn-out process with no successful outcome. This is despite the fact that our law recognises that cases such *SR v Facebook Inc* should have a simple remedy for the victim, such as companies like Facebook releasing the information to law enforcement under Court Order, rather than prolonging a victim's anxiety and suffering with no result.

Despite agreeing that the applicant was entitled to the information, Facebook still refused to provide it to her unless it was obtained through a valid legal process. Cyber harassment often means not being able to identify the perpetrator; or establishing a sufficient causal nexus between the harassment and a suspected perpetrator.

The mechanisms in our current legislation, especially those created by the Cyber Act, may assist future applicants in being able to request the information. If a court is satisfied that a protection order must be issued and the particulars of the perpetrator, or the electronic communications service provider, are unknown, a court may issue a directive to the electronic communications service provider to furnish such particulars to a court by means of an affidavit that may identify a perpetrator.¹⁰⁹ The Cyber Act further empowers the court to make an assessment on whether or not the electronic communications service provider is in a position to: remove the data message or a link to such data message; or disable access to the data message or a link to such data message.¹¹⁰ However, as is usually the case without economic resources or education on the processes to follow in terms of legislation, many victims will not be able to access the remedies available to them.

VI INTERACTION BETWEEN SOUTH AFRICAN POLICE SERVICES AND COURTS

¹⁰⁹ Section 21 of the Cyber Crimes Act 19 of 2020.

¹¹⁰ Ibid note 109 at Section 21(VI).

Even the Cyber Act, with all its intentions to modernise such protections, is still ultimately reliant on the SAPS and our local Courts to enforce such protections. Section 4 of the PHA gives a victim the opportunity to try and identify the perpetrator by calling on the SAPS to investigate, and compelling internet service providers to furnish the SAPS with necessary information (this is intended to relieve the burden from the victim of proving a *causal nexus* and place it on the SAPS). Section 6 of the PHA empowers the SAPS to ascertain the name and address of a perpetrator to assist tracing agents. Unfortunately, if the SAPS put their hands up and do not assist victims, neither the PHA nor the Cyber Act impose any consequences on the SAPS for failing to comply with a court order directing them to investigate. The writer is of the view that if specialist training is provided to members of the SAPS, this might empower them to assist in matters of cyber harassment. Further, the majority of SAPS precincts do not have any experience in investigating cybercrimes, and for the most part, their own electronic systems are not in working order.¹¹¹ It is rare for the SAPS to get involved or provide meaningful assistance when cyber harassment occurs.¹¹²

Further logistical issues are being added onto the SAPS - the Cyber Act now deals with cyber harassment and cyberstalking. Notwithstanding the enactment of the Cyber Act, there is a real risk that the issues surrounding harassment may be circumvented, in that the Cyber Act might undermine the remedies provided for in the PHA. It is up to our Courts, despite dealing with matters on a case-by-case basis, to focus on the individual pieces of legislation rather than dealing with harassment, as a whole. The Cyber Act provides temporary solutions but does not address the root of the problems. Similarly, the PHA, on its own, provides victims of cyber harassment with the ability

¹¹¹ Only in July 2022, did the SAPS publish a revised version of the Standard Operating Procedures (SOPs) for the investigation, search, access, or seizure of electronic evidence in terms of the Cybercrimes Act.

¹¹² The writer is of the view that an online solution could offer an unbiased method that can help resolve disputes either through a web-based forum which allows applications and respondents to attempt to resolve their differences on their own or if necessary, the use of a professional.

to obtain a protection order - but a protection order is essentially an interdict and is '*not a real punishment or preventive measure*'.¹¹³

The Cyber Act, through the South African Courts, needs to find harmonisation with the PHA, to empower a victim of cyber harassment to seek a protection order in addition to laying a criminal complaint. A court can also grant an order directing an ECSP to take specific action in order to combat the crime complained of. ISPs now have an obligation to retain information relating to cybercrime to assist police in their investigation and should they fail to comply, can be liable to a fine of up to R 50 000.00. Where the Cyber Act can carry weight over the PHA, is that the Cyber Act provides the SAPS with authority to not only investigate, search, access and seize, but also to cooperate with foreign states to investigate cybercrimes. Foreign states, especially the US and the EU, are more advanced in dealing with Cyber Crimes, and where the Cyber Act allows for cooperation, local authorities may benefit from cases that are similar in nature and that have already been investigated and prosecuted by foreign states. The Cyber Act further affords South African courts with jurisdiction to adjudicate over any act or omission alleged to constitute an offence under the Cyber Act and affect a person in South Africa, even in instances where such a defined cybercrime is committed outside of South Africa.

VII INTERNATIONAL TRENDS

In the United States, there is no clear definition of what constitutes cyber harassment. In many US states, legislators have attempted to address the issue of increased cyber harassment by adding wording to existing harassment legislation, thus extending it to when the harassment takes place on an online medium. Other states have attempted to institute legislation specifically directed to combat cyber harassment.

¹¹³ Bliss, L (2019) The Protection from Harassment Act 1997: Failures by the Criminal Justice System in a Social Media Age (looks at UK's Protection from Harassment Act).

Worldwide, cyber harassment has not been properly defined, as it is not as simple to identify as traditional stalking or harassment (which normally entails a person being physically present when partaking in or causing the harassment).

In 2013, the New York Police Department obtained an arrest warrant against a woman based in New Zealand for stalking and terrorising a woman based in New York. The case shows that no legislation can be drafted on the traditional understanding of harassment and stalking.

The following are key differences between ordinary harassment and cyber harassment: a message communicated online can be sent to anyone with internet access, is present immediately, and cannot be taken back or deleted; the stalker may be anywhere in the world; the stalker can stay anonymous with ease because of the lack of physical contact involved in this crime; the stalker may easily impersonate another person to communicate with the victim, and the stalker may use third party individuals to contact or communicate with the victim.¹¹⁴

The above list demonstrates how cyber harassment can be regarded as a crime that is unlike ordinary harassment and should thus be dealt with differently in the legislation. Such unique legislation must specifically address obstacles such as VPN and server proxies that make identifying the perpetrator difficult and implement mechanisms to overcome such obstacles.¹¹⁵

Harassment on the Internet can take a variety of guises. A direct form of cyber harassment may involve the sending of unwanted emails which are abusive, threatening, or obscene from one person to another. It may involve electronic sabotage in the form of sending the victim hundreds or thousands of junk email messages (an

¹¹⁴ Online Harassment: A Research Challenge for HCI, Jennifer Golbeck.

¹¹⁵ Cyber-stalking: the Regulation of Harassment on the Internet, Yaman Akdeniz Criminal Law Review, 1998.

activity known as ‘spamming’) or sending computer viruses. Indirect forms of harassment may involve a cyberstalker impersonating his/ her victim online and sending abusive emails or fraudulent spam in the victim's name. Victims may be subscribed to a number of mailing lists with the result that they receive hundreds of unwanted emails every day, without them knowing. One victim of cyber-stalking in the United States, Cynthia Armistead, received thousands of offensive telephone calls after her stalker posted a fake advertisement on a Usenet discussion group, offering her services as a prostitute and providing her home address and telephone number.

In Australia, specific legislation is absent and cyber harassment is treated as a criminal offence. The Criminal Code Act 1995 (Commonwealth) criminalises the use of a phone or the internet to threaten, harass, or seriously offend somebody.¹¹⁶ Section 13 of the Crimes (Domestic and Personal Violence) Act 2007 (NSW) criminalises stalking. Despite the legislation in Australia, only around 2010 did Australia have its first prosecution in Cyber Harassment and show that it is possible to achieve a successful conviction of a perpetrator. In April 2010, Shane Phillip Cerado admitted to sending his best friend vicious and threatening messages. The recipient ended up taking his own life. Cerado received an eighteen month community based order.¹¹⁷

The idea of distinct borders separating domestic and international communications has been eroded, and 2022 onwards will see the promotion of Web3. The Metaverse combines multiple elements of technology, including virtual reality, augmented reality and video, where users ‘live’ within a digital universe.

US laws often require that the harm be physical or ‘real’ – which may not extend to email threats. Unlike in the US, the PHA specifically includes psychological distress (along with economic, mental or physical harm) in its definition.

¹¹⁶ Section 474.17 of the Criminal Code Act, 1995 (Commonwealth).

¹¹⁷ Lauren Wilson, ‘Cyber bully convicted,’ The Australian, 9 April 2010.

VIII CONCLUSION

Often the perpetrators are geographically dispersed, unidentifiable, and cannot be located. The internet provides anonymity and no penalty for egregious behaviour on it.

All the research clearly shows that cyber harassment is increasing at a high pace and has devastating effects on its victims, who are the receiving end of those who use systems for ulterior motives. Further legal regulation and developments are required to curb suicide incidents, and economic and psychological harm.

An effective solution or defence against cyber harassment requires effective international cooperation in criminal matters. Hence, the question is: does the PHA afford an applicant with sufficient protection, in light of the increasing number of cybercrime and harassment cases? Does the Cyber Act meet international standards?

The PHA should be more than a preventative measure and the Cyber Act should be more than simply criminalising unlawful conduct.¹¹⁸ Unfortunately, there is a disconnect between the procedures provided for prevention, detection and investigation methods utilised. Both the PHA and Cyber Act should be utilised in conjunction. Measures must be put in place, possibly through future regulations, that require better intervention from service providers both locally and internationally. As an example, in the European Union service providers will only provide simple information on receipt of a Court Order and/or Subpoena from the SAPS. Unfortunately, enlisting the services of the SAPS to actually provide these services is at times an insurmountable obstacle, or at least an expensive obstacle. It is required for the various State Departments, from the Department of Education, the Department of

¹¹⁸ Watney, MM. 'Cross-Border Law Enforcement: Gathering of Stored Electronic Evidence.' *Journal of Information Warfare*, vol. 15, no. 3, 2016, pp. 69–80. JSTOR.

Justice, to the Minister of Police, to develop a new uniform approach within the confines of the PHA and Cyber Act. Currently, the PHA seems to be ‘oblivious’ to these kinds of obstacles – it empowers SAPS to investigate but does it consider that identifying a perpetrator can be near impossible.

Social media sites are attempting to assist in the fight against cyber harassment, but they don’t seem to be taking it too seriously and blur the lines as to what their rules believe constitutes online abuse and cyberbullying. The advice promoted by social media sites is to unfollow and end any communication with abusive accounts and thereafter if the behaviour continues, it is recommended that the abuser’s account is blocked and reported through the internal mechanisms of the social media platform.

Social media platforms should play a major role in combating cyber harassment by not only providing victims an opportunity to report such abuse but also by playing a pivotal role in educating users that such options exist prior to having the victims having to report the matter to the SAPS. Similar procedures to what eBay has done with its online dispute resolution system should be put in place.¹¹⁹

The current South African legislation, despite the enactment of the Cyber Act, is insufficient to deal effectively with cyber harassment. There needs to be a harmonisation of the legislation, which can be achieved through the creation of a central reporting forum – not simply an ombudsman – to assist with recourse for victims and to aid the SAPS with the implementation of protections offered by the Cyber Act and the PHA.

¹¹⁹ eBay Services: Buying and Selling Tools: Dispute Resolution Overview, <https://pages.ebay.com/services/buyandsell/disputeres.html> accessed on October 29, 2022.

An additional recommendation would be the upskilling of the SAPS, through the establishment of a specialist unit that receives training in modern techniques to combat and prevent cyber harassment.

The Cyber Act alone does not amplify the remedies offered by the PHA other than creating specific penalties. It is essential for all stakeholders to collaborate. Although it can be argued that the PHA may be able to keep pace with the latest developments in social media and technology, it is likely to be more effective in addressing cyber harassment through collaboration with social media platforms, service providers, and the upskilling of all stakeholders.

Bibliography

Articles

- A. Mmabthao, South African Police Service capacity to respond to cybercrime: challenges and potentials, Journal of Southwest Jiaotong University.
- Ellison, L., & Akdeniz, Y., “Cyber-stalking: the Regulation of Harassment on the Internet,” [1998] Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet.
- Governance, Public Safety and Justice Survey (GPSJS) Victims of Crime 2020/21, Risenga Maluleke, Statistician-General.
- Valentina Beghini, Violence and harassment in the world of work: A guide on Convention No. 190 and Recommendation No. 206 International Labour Office – Geneva: ILO, 2021.

Books

- Aharon Barak, Human Dignity The Constitutional Value and the Constitutional Right, pp. 103 – 113.
- C.R Snyman, Criminal Law, Edition, 5; Publisher, LexisNexis, 2008.
- CB Prest. The Law and Practice of Interdicts, 1996.
- Christopher Enders, Right to have Rights – The German Constitutional Concept of Human Dignity, Volume 3, Issue 3 (2010).

Case Law

- *Bernstein and Others v Bester NO and Others* (CCT23/95) [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (27 March 1996).
- *De Reuck v DPP* 2004 (1) SA 406 CC.

- *Gouws v De Lange and Another* (2842/14, 3449/14, 3450/14) [2014] ZAECPHC 89 (11 December 2014).
- *Gouws v De Lange and Another* (2842/14, 3449/14, 3450/14) [2014] ZAECPHC 89 (11 December 2014).
- *H v W* (12/10142) [2013] ZAGPJHC 1; 2013 (2) SA 530 (GSJ); 2013 (5) BCLR 554 (GSJ); [2013] 2 All SA 218 (GSJ) (30 January 2013).
- *Mnyandu v Padayachi* (AR162/2014) [2016] ZAKZPHC 78; [2016] 4 All SA 110 (KZP); 2017 (1) SA 151 (KZP) (1 August 2016).
- *RKM v RLB* case no: 10175/2013.
- *S v Makwanyane and Another* (CCT3/94) [1995] ZACC 3; 1995 (6) BCLR 665; 1995 (3) SA 391; [1996] 2 CHRLD 164; 1995 (2) SACR 1 (6 June 1995).
- *S v Trainor* 2003 (1) SACR 35 (SCA).
- *S v Trainor* 2003 (1) SACR 35 (SCA).
- *SATA WU obo Dlamini v Transnet Freight Rail, a Division of Transnet Ltd and Another* [2009] JOL 24429 (Tokiso).
- *Silberberg v Silberberg, Silberberg v Silberberg and Another* (A 603/2007, 4581/2008) [2013] ZAWCHC 5 (29 January 2013).
- *SR VS Facebook Inc* 2020/14827 28 July 2020.
- *Van der Berg v Coopers & Lybrand Trust (Pty) Ltd and Others* (466/98) [2000] ZASCA 73; 2001 (2) SA 242 (SCA) ; [2001] 1 All SA 425 (A) (29 November 2000).

Convention

- Violence and harassment in the world of work: A guide on Convention No. 190 and Recommendation No. 206 International Labour Office – Geneva: ILO, 2021

Legislation

- The Criminal Code Act, No 12, 1995 (Commonwealth).
- Criminal Procedure Act 51 of 1977.
- Criminal Law (Sexual Offences and Related matter amendment Act), Act 13 of 2021.
- Copyright Act 98 of 1978, as amended.
- Cybercrimes Act 19 of 2020.
- Magistrate's Court Act 32 of 1944.
- The Uniform Rules of Court.
- The Constitution of the Republic of South Africa, Act 108 of 1996.
- Domestic Violence Act 116 of 1998.
- Protection of Harassment Act 17 of 2011.
- Films and Publication Amendment Act 11 of 2019.
- EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
- Electronic Communications and Transactions Act 25 of 2002.
- Mogale S et al: Violence Against Women in South Africa: policy Position and Recommendations, 2012.

Websites

- 'Facebook Horizon | Oculus.' Wwww.oculus.com, www.oculus.com/facebook-horizon/.
- 'Local NGO Assists Schools and Parents with Anti-Bullying Skills after Limpopo-Tragedy.' Parent, www.news24.com/parent/learn/teacher-collection/local-ngo-assists-schools-and-parents-with-anti-bullying-skills-after-limpopo-tragedy-20210419. Accessed 29 Oct. 2022.

- ‘Are Your Hands Tied When It Comes to Cyber Harassment?’ De Rebus, 31 Aug. 2018, www.derebus.org.za/are-your-hands-tied-when-it-comes-to-cyber-harassment/. Accessed 29 Oct. 2022.
- ‘eBay Services: Buying and Selling Tools: Dispute Resolution Overview.’ *Electronics, Cars, Fashion, Collectibles & More / EBay*, <https://pages.ebay.com/services/buyandsell/disputeres.html>. Accessed 29 Oct. 2022.
- ‘Mark Zuckerberg Says Meta’s Metaverse Project Will Lose ‘Significant’ Sums of Money for up to 5 Years.’ Finance.yahoo.com, finance.yahoo.com/news/mark-zuckerberg-says-metas-metaverse-095455570.html.
- ‘Social Media Use during Coronavirus (COVID-19) Worldwide.’ Statista, www.statista.com/topics/7863/social-media-use-during-coronavirus-covid-19-worldwide/#dossierSummary_chapter2.
- 5 Ct. Uncourt 10 (2018), Legalities of Using Virtual Private Network accessed at <https://heinonline.org/HOL/LandingPage?handle=hein.journals/counco5&div=147&id=&page=>. Accessed on 8 January 2022.
- Metaverse: another cesspool of toxic content accessed at https://www.sumofus.org/images/Metaverse_report_May_2022.pdf. Accessed on 4 June 2022.
- Rachel Metz, ‘Meta is giving avatars a four-foot buffer zone to cut back on VR harassment’ available at <https://edition.cnn.com/2022/02/04/tech/meta-vr-avatar-safety-boundary/index.html>. Accessed on 04 February 2022.

Journal Articles

- Smit, DM. 'Cyberbullying in South African and American Schools: A Legal Comparative Study.' *South African Journal of Education*, vol. 35, no. 2, 31 May 2015, pp. 1–11, 10.15700/saje.v35n2a1076. Accessed 29 Oct. 2022.
- Walker, Carol M. 'Developing an Understanding of Cyberbullying.' *Teacher Education for Ethical Professional Practice in the 21st Century*, pp. 236–259, 10.4018/978-1-5225-1668-2.ch011. Accessed 29 Oct. 2022.
- Kift, Sally; Campbell, Marilyn; Butler, Des --- 'Cyberbullying in Social Networking Sites and Blogs: Legal Issues for Young People and Schools' [2010] *JILawInfoSci* 13; (2010) 20(2) *Journal of Law, Information and Science*.
- A. Srivastava, J. Boey: *Online Bullying and Harassment*, 2012.
- Bliss, Laura. 'The Protection from Harassment Act 1997: Failures by the Criminal Justice System in a Social Media Age.' *The Journal of Criminal Law*, 6 Feb. 2019, p. 002201831982926, 10.1177/0022018319829262.
- Celuch, Magdalena, et al. 'Individual Factors Predicting Reactions to Online Harassment among Finnish Professionals.' *Computers in Human Behavior*, vol. 127, Feb. 2022, p. 107022, 10.1016/j.chb.2021.107022. Accessed 9 Dec. 2021.
- Chik, Warren, *Harassment through the Digital Medium A Cross-Jurisdictional Comparative Analysis on the Law on Cyberstalking*, *Journal of International Commercial Law and Technology*, 2008.
- Huang, Yun-yin, and Chien Chou. 'An Analysis of Multiple Factors of Cyberbullying among Junior High School Students in Taiwan.' *Computers in Human Behavior*, vol. 26, no. 6, Nov. 2010, pp. 1581–1590, 10.1016/j.chb.2010.06.005.
- Golbeck, J. (2018). *Online Harassment: A Research Challenge for HCI*. In: Golbeck, J. (eds) *Online Harassment. Human–Computer Interaction Series*. Springer, Cham.
- Sulfab, M. 'Challenges of cybercrime in South Africa' *American University* 2004.

- Walker, C.M (2014), Cyberbullying redefined: An analysis of intent and repetition. *International Journal of Education and Social Science*.
- Watney, MM. 'Cross-Border Law Enforcement: Gathering of Stored Electronic Evidence.' *Journal of Information Warfare*, vol. 15, no. 3, 2016, pp. 69–80. *JSTOR*, <https://www.jstor.org/stable/26502745>. Accessed 29 Oct. 2022.

