Children's Right to Digital Safety: Evaluating the way by which the law can increase effective protection for children in South Africa

Submitted in partial fulfilment of the requirements of the Master of Laws in Multidisciplinary Human Rights

By

Matikomborera Nyamadzi (u1702663)

Prepared under the supervision of

Dr Elvis Fokala

Faculty of Law, University of Pretoria, South Africa

30 December 2023

Plagiarism Declaration

I, Matikomborera Nyamadzi (u17020663), declare as follows:

1. I understand what plagiarism entails and am aware of the University's policy in this regard.
2. This mini-dissertation is my own, original work. Where someone else's work has been used (whether from a printed source, the internet or any other source), due acknowledgement has been given and reference made according to the requirements of the Faculty of Law.
3. I did not make use of another student's work and submit it as my own.
4. I did not allow anyone to copy my work with the aim of presenting it as his or her own work.

Signature: *M.Nyamadzi*

Date: **29 December 2023**

Dedication

This work is for the children whose needs are not fully understood and therefore not adequately protected, may your voices and needs find protection.

Acknowledgements

This work could not have been completed without the support of the Mastercard Scholarship Foundation. Not only did the scholarship offer me financial support but also a family to call my own and help me walk my Masters Journey.

Thank you to Dr Isike whose office became my place of solace and motivation. To my food group, Abigail Mberi and Randy Seda, those late nights and constant pushes helped me make it to the end, Thank you!

To my Husband, Dr Taruvinga, thank you for taking on an academic area you knew nothing about and helping me make it the best I could. You have been the best editor and proofreader anyone could have asked for.

But most important in my journey has been my supervisor, Dr Fokala. You single handedly pushed me to the finish line, especially when I lost sight of it. Thank you for ensuring that I would cross it and see the other side of the master's degree. Your knowledge and 6am calls have paid off. Thank you!

Table of Contents

Acronyms and Abbreviations

African Childrens Charter	African Charter on the Rights and Welfare of the Child
AU	African Union
Commission	African Commission on Human and Peoples' Rights
Committee	African Committee of Experts on the Rights and Welfare of the Child
UNCRC	United Nations Convention on the Rights of the Child
CSAM	Child Sexual Abuse Material
GDP	Gross Domestic Product
GCI	Global Children Initiative
BBC	British Broadcasting Corporation
POPIA	Protection of Personal Information Act
ECTA	Electronic Communication and Transactions Act
MDG	Millennial Developmental Goal
SDG	Sustainable Developmental Goal
AM	Algorithmic Manipulation
GCIS	Government Communications and Information System
CIL	Customary International Law
Malabo Convention	African Union Convention on Cyber Security and Personal Data Protection

Chapter 1: Background of the Study

1. Introduction

In the age of the internet of things, online presence is becoming a social norm. Research has shown that children, specifically those between the ages of 15 and 18, make up the majority of the online population.[1] Coming up closely behind them, with a growing online presence are children between the ages of 7 to 10.[2] The nature of the internet is such that it has increased opportunity and risk simultaneously. For children, the harms and risks are predominantly predative risks. Statistics show that the greatest risks and harms usually experienced by children online, are as Child Sexual Abuse Material (CSAM).[3] This, however, does not eliminate other harms such as identity theft, bullying, shaming, harassment, and exploitation. And the common link between all these harms and the corresponding harm facts, is the exposure and access children have to the internet.

It is common cause that children's exposure to these online harms and risks has also been exacerbated by increased screen time. According to Gottschalk, writing in 2019, Children between the ages of 8 to 18 in countries with higher internet access rates, spend on average between 7 to 8 hours per day, online.[4] These countries, are predominantly countries where there is a higher Gross Domestic Product (GDP) and better access to both the devices for use and the internet for surfing.[5] Specifically at the African regional level, children's internet penetration reached an exponential peak during the implementation to the non-pharmaceutical measures to curb the adverse effect of COVID-19. [6] During these times, as it is now known, everyone including

[1] International Telecommunication Union (2016), "Measuring the Information Society Report".
[2] Same as above.
[3] Internet Watch Foundation, Annual Report, 2022.
[4] F Gottschalk, 'Impacts of technology use on children: Exploring literature on the brain, cognition and well-being' 2019 *OECD Education Working Paper* No. 195.
[5] In comparing various European countries, Guštin notes that besides the impediment that may be resources and access to the internet, there is also the added layer of language barriers that may limit how different countries and communities are able to use the internet as a tool for development. See Guštin M 'Challenges of protecting children's rights in the digital environment' (n.d.) 6, *EU and Comparative Law Issues and Challenges Series* (ECLIC) 453-486, 465.
[6] Human Rights Watch 'Impact of Covid-19 on Children's Education in Africa' available at https://www.hrw.org/news/2020/08/26/impact-covid-19-childrens-education-africa (accessed August 3, 2023).

children, were expected to spend more time at home, attend classes online and socialise online instead of meeting with their friends in schools as it had always been for them. South Africa was one of the most affected and 'locked-down' African countries.[7] Notwithstanding, that the increased trend of children's access to the internet had already shown signs before COVID-19.

In 2019, the Global Children Initiative (GCI) established that 88% of teenagers (children of ages 12 to 18) in South Africa had access to smart phones with internet capability.[8] Their involvement in the digital world offers multiple benefits to them, such as opportunities for learning, networking, access to information and expression in ways they would not have attained without access to the internet and technology.[9] However, access to this opportunity for these children, their active presence on the internet, especially on social media platforms, also exposes them to a range of serious online dangers, including, cyberbullying, grooming, threats, blackmail, sexual harassment, sexual exploitation and hate speech.[10] These dangers have profound consequences, jeopardising children's well-being, and development and in some instances, it could lead to the child victim committing suicide.

Although access to the internet and smart devices is on the rise in Africa and more so in South Africa, there is still a disparity in the forms of harm that the children across the globe are more likely to face. The harms that children in South Africa face, will most likely be similar to those of children in the global north because of the comparatively higher household income in South Africa than the rest of the sub-Saharan region.[11] However, there are also factors of socio-economic relevance that will also impact how this experience will play out. Examples of these factors could include literacy rates, economic inequalities, amongst other region, specific issues.

---

[7] For more on this, please visit the South African Government website on Corona Virus restrictions - available at https://www.gov.za/Coronavirus, (accessed 17 August 2023).
[8] 'Growing up in a connected world' UNICEF Office of Research – Innocenti, Florence, 2019.
[9] Guštin, n5 above, 456.
[10] Guštin, n8 above, 454.
[11] When comparing the economy of South Africa with the rest of the continent, its economy is bigger and the access to internet corelates with the size of the economy. See https://www.trustonic.com/opinion/what-are-the-barriers-to-smartphone-expansion-across-africa/#:~:text=In%20certain%20regions%20of%20Africa,all%20nations%20on%20the%20continent (accessed 16 August 2023).

The internet exists in the larger framework of global issues, this means intersectional issues that affect children offline, will be translated or adapted on the internet. The geopolitical and economic climate of a region affects the extent to which a child can access the internet. Different groups of children are exposed differently to online harms. For example, children in particular regions are exploited through interaction with predators online, whilst another group are exploited by being put online for other predators' consumption.[12] Therefore, as a result of factors such as geopolitical vulnerabilities, any discussion of digital insecurity for a child in Africa will differ to that of a child in either the global West, or the East.

For example, in 2020, in a Malawian village, *Njewa* near Lilongwe, a Chinese man recruited village children to have them act out skits where they used racial slurs and call themselves demeaning terms.[13] The purpose of this footage was to entertain Chinese viewers and exploit the children for profit. This was just an example of which was broadcasted by the British Broadcasting Company (BBC)to be a growing market in China for personalised videos featuring unknowing victims.[14] In this instance, as a result of lack of knowledge and access to the internet to understand the effect of the videos, the children's right to dignity was deeply affected.

In a different, but, comparable instance, in 2021, the suicide case of Lufuno Mavhunga in Limpopo, South Africa was tragic. This case brought to the spotlight the ripple effects of the dangers faced by children online.[15] Although online bullying is statistically rampant, globally, in South Africa, the phenomena was not as prevalent or well covered until Lufuno's untimely passing spotlighted its severity.[16] In this case, the

[12] Skelton and Mezmur write about the recommendations proffered to various states by the UNCRC and note how the Philippines'' comments were also unique in that the state had higher levels of webcam abuse wherein children are being abused and exploited for the purpose of entertaining adults in other regions of the world. Though this is not statistically proven through research, I argue that it is reflective of a noticeable trend amongst types of crimes and the regions they occur in. however, this is not the focus of the study and as such is to be noted for further reading. See A Skelton & B D Mezmur 'Technology Changing @ a Dizzying Pace: Reflections on Selected Jurisprudence of the UN Committee on the Rights of the Child and Technology' (2019) 3(3) *Peace Human Rights Governance* 275-305.
[13] 'Racism for sale' BBC Africa Eye documentary, available at https://www.bbc.com/news/av/world-africa-61764466 accessed 16 August 2023.
[14] BBC Africa, n13 above.
[15] Daily Maverick, Bullied Limpopo schoolgirl's suicide raises disturbing questions about moral compass of our children, M le Cordeur, May 2021.
[16] Shumba K et al "Chanting for social change: An analysis of Makhadzi's song Muvhili Wanga (Tribute

young grade 10 pupil suffered physical bullying which was taken to online platforms, such as Tik Tok and Instagram, by fellow pupils. The online bullying included both the virality of the footage of her being physically assaulted as well as threats of continued violence. With exposure to the abusive and slanderous material, Lufuno's mental well-being was affected, and eventually led to her taking her life. The case sparked outrage in South Africa, for the upsetting loss of life but more so the danger of digital safety of children. Lufuno's story was no different. As is the case in sensational media, discussion is sparked about the questions beyond the issue, and in this case, how to protect children and teach responsible internet presence.

Online bullying thrives because it often goes undetected. Common to both the cases of Lufuno and the Malawian children, is that the algorithms kept the information out of mainstream circulation and therefore made it go undetected for a while. The information circulated amongst a select group of people to the exclusion of others, through the work of content curating algorithms. Key to establishing digital safety is the issue of understanding algorithms. Understanding the way in which algorithms work will enable policies to be relevant and better suited to addressing digital safety. With the correct knowledge of algorithm functions and impacts, states are more likely to better address the issues on hand.

Until the promulgation of the Protection of Personal Information Act (POPIA)[17] and the Cyber Crime Act,[18] the Electronic Communications and Transactions Act (ECTA)[19] was the only Act available to deal with matters arising from online interaction. It addressed both regulation of online communication and transactions, as well as identifying cybercrimes and their penalties. However, the central objective of the ECTA's is to provide regulation for persons communicating and transacting online.[20] This means that its scope is limited and was inadequate to cover all forms of exposure. Though aspirational in its objectives, ECTA is formulated in a way that leaves a gap when it comes to extensively protecting and addressing technology related safety

to Lufuno) and the scourge of school cyberbullying in South Africa" (2023) 6:1 *Journal of African Films & Diaspora Studies.*
[17] Act 4 of 2013.
[18] Act 19 of 2020.
[19] Act 25 of 2002.
[20] ECTA, preamble.

issues, more particularly cybercrime as we know it in the modern age. The introduction of the Cybercrime Act sought to fill this legal gap and present better protection for South Africans whose online presence is ever growing. Through the introduction of POPIA, a new page was turned on legal protection for privacy rights. Because of this, the question of using the law as a protection tool has also come under scrutiny. But the question remains, the harms faced online by children, are they being sufficiently protected by the laws that exist, both through black letter law and policy reforms. As elaborated further below, the central concern of this research is to scrutinise the sufficiency of existing, South African national laws in safeguarding the rights of children during their interaction with the internet and technology.

2. Problem statement

The rapid advancement in technological inventions has significantly increased the accessibility, usage, and exposure to the internet across varied age groups. Children are now the most active internet and technology users. As indicated earlier they use it, frequently, far beyond adults, on social media sites such as Facebook, TikTok, Instagram, online gaming, and other video-sharing platforms. This usage, while productive in enabling and enhancing children's development, it has increased children's susceptibility to unsafe online interactions. Although South Africa has legislation designed to protect users; incidents of internet abuse/harmful contact are significantly widespread, which could signify legislative loopholes/inadequacies. The number of dangers faced by children, during their interaction with the internet and technology, is already a matter of concern. States, especially state parties to the United Nations Convention on the Rights of the Child (UNCRC)[21] and the African Charter on the Rights and Welfare of the Child (African Children's Charter)[22] are increasingly required to adopt both legal and other measures at the national level, to circumvent the dangers children's face online.

South Africa acceded to the UNCRC in June 1995, and to the African Children's Charter in January 2000. Even though, the state has demonstrated its commitment to these treaties by enacting various South African domestic laws relating to and

[21] Adopted 20 November 1989, entered into force 2 September 1990, 1577 UNTS 3.
[22] Adopted 11 July 1990, entered into force 29 November 1999, CAB/LEG/24.9/49 (1990).

protecting children in the country, there seems, as demonstrated in this research, that there is not enough coverage, in law, of the children's online rights and dangers. Therefore, an examination of the effectiveness of current laws is crucial and will, to a very large extent, look to avenues that can inform the state of the next steps it should take to strengthen its coverage and protection of children's rights. Thus, the main objective of this dissertation is to examine the extent to which laws ensure children's online safety and to proffer advocacy and multidisciplinary approaches to improving the safety mechanisms in place.

3. Research Objectives

1. To examine gaps in South Africa's legal provisions on child online safety.
2. To assess the impact of the regional human rights system on child online safety in South Africa.
3. To offer strategic advocacy and litigation recommendations for bridging the gap between the exposure to harm and the effective protective laws.

4. Research questions

The main research question this mini dissertation seeks to respond to is:

To what extent could the law be more effective and responsive as a tool for ensuring child online safety in South Africa?

The research sub-questions that flow from this main question are:

1. What are the harms faced by children online in African contexts that call for more specific forms of protection?
2. How has South Africa addressed children's digital safety?
3. How does the regional international human rights system, specifically the AU, address children safety online; and
4. Beyond the black letter law, how can strategic litigation and advocacy aid in creating effective law and protection?

5. Literature review

The research and discourse surrounding the right to digital safety of children is mired with multiple views and approaches. Several scholars have written on, and dissected the challenges posed by the growing impact of the internet on children's rights The UN Committee on the Rights of the Child, issued General Comment 25 which was a turning point in international human rights law for the protection of children's digital rights.[23] In General Comment 25, the Committee outlines six areas of children's rights in the digital environment, which are investigated more substantively:

1. Civil rights and freedoms (VI);
2. Violence against children (VII);
3. Family environment and alternative care (VIII);
4. Children with disabilities (IX);
5. Health and welfare (X);
6. Education, leisure, and cultural activities (XI).

At the inception of the UNCRC, the internet and digital age was not even a fraction of what it is today. And so, we rely on the work of the Committee which allows for scholarship on the UNCRC to be developed towards a post digital era and takes into cognisance scenarios and cases of the time. However, because the comments do not form part of, hard law, they still require regional bodies and states to incorporate them in National laws to enable their enforcement. In essence, what the Committee produces through the comments are persuasive guidelines that help to formulate better and cohesive laws for the protection of children.

Of specific concern to South Africa, is the point stressed at paragraph 60 of the General Comment; wherein an active obligation is placed on States to protect children from third-party interference where they make use of their freedom of expression, and mentions "cyberaggression, and threats, censorship, data breaches and digital surveillance." This particular note and discussion will be pertinent in unpacking digital unsafety as there is need for there to be a balance between interference for protection

[23] General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25.

and non-interference for the purposes of respecting and enabling children to enjoy their digital rights.

Privacy both as a right and as a core principle has been the guiding objective for how the scholarly literature surrounding children has been developed around article 10. In article 10 of the African Children's Charter,[24] a child is guaranteed privacy and autonomy. In this context of digital presence, this should include autonomous decision making and exploration of technology. Indeed, all this must occur within the framework of the best interest of the child, however, the question left unanswered especially for the context of South Africa, is where and how the law can help to create safety without infringement of the child's rights, especially during their interaction with technology and the internet.

Leading scholarship on the use of law as a tool for creating safe and efficient regulation of digital interaction converges and begins on the eminent point that there is insufficient regulation of the digital space.[25] The digital space is largely left to the care of parents and guardians to regulate for their children. In some spheres, an argument exists that children by virtue of being presumed as technologically advanced, and sometimes more than adults, should be allowed to self-regulate.[26] However, what this view fails to consider is the enormity of the dangers that the system or the digital space is designed to expose children to. This is whether or not the children are tech savvy.[27] For the South African child, the risk is more apparent because of the digital inequality brought about by low literacy rates.[28] These low literacy rates also contributes to the lack of education in safe use of the internet.

In writing about the growth of internet use amongst children, Livingstone argues that a pattern that was taken in the regulation of the global north's tech boom, is being copied by the global south and will result in eminent failure.[29] She argues that allowing the internet and its discovery by all, including children, to be played out as a free

[24] Article 10, African Children's Charter.
[25] S Livingstone 'Children's digital rights: a priority.' (2014) 42 *Intermedia*, 20-24.
[26] E Lievens 'Growing Up with Digital Technologies: How the Precautionary Principle Might Contribute to Addressing Potential Serious Harm to Children's Rights,' (2021) 39:2 *Nordic Journal of Human Rights*, 128-145.
[27] Livingstone, n25 above at 22.
[28] Hart S A 'Identifying the factors impacting the uptake of educational technology in South African schools: A systematic review' (2023) 43:1 *South African Journal of Education* 1-16.
[29] Livingstone, n25 at 21.

market can lead to serious consequences.[30] She calls on the regulation of the digital environment in the global south, by way of including and involving children, but also promoting safety by design.[31] South Africa, being a part of the global south has played into this narrative through the development of laws that are intended to bring safety in the use, but not design of technology. Further, its processes have thus far, greatly, lacked in the inclusion of children.

Lievens encourages precaution in development of safety by design. [32] In his writing, he says that by way of applying the precautionary principle and pre-empting harm, any policy and legal outputs of a state will better protect children's presence online.[33] This approach is premised on things like equal access to the internet, and even more so internet literacy. As earlier mentioned, South Africa has struggling literacy rates that would not bode well with a copy paste approach of the precautions that would be otherwise anticipated in a more developed nation.[34] Ultimately, Lievens' suggestion allows the application of human rights as a cornerstone of the realisation of safety legislation for children in digital space, but negates the input required from states starting from a different footing than that of global north states, in this case grassroot issues of literacy.

Stadniczeńko brings a more wholistic approach. He factors the issue of region specificity in by taking a more wholistic approach to the issue and couches the development of legal solutions by first unravelling the phenomena that needs to be remedied.[35] He narrates the threats and the possible solutions, which as he offers is the transparency of data collection and storage. By so doing, he proffers that regulation of what is collected and stored, gives back the power to the users of the internet to better choose how their data and digital presence can be regulated. This is approach maximises autonomy. However, it does not consider the issues surrounding younger children and the skill set required to understand the power of the tool given.

[30] Livingstone, n25 above at 22.
[31] Livingstone, n25 above at 22.
[32] Lievens, n26 above at 128.
[33] Lievens, n26 above at 128.
[34] Hart, n28 above at 3.
[35] D. Stadniczeńko 'Children's Rights in the Digital Environment under the Convention on the Rights of the Child' (2022) 15:2 *Teka Komisji Prawniczej PAN Oddział w Lublinie,* 321–331.

Thus, the literature at large, offers macro level solutions and allows for the development of similar but not very effective solutions. The solutions currently available do very little to account for specific sets of facts, but even generally for African leaning facts. As such, this research seeks to weave together the existing research, to contextualise it and to bring together solutions that will enrich the proposed solutions for South Africa.

6. Methodology

This mini-dissertation adopts a legal doctrinal method of research, couched in a children's-rights based lens. A children's rights lens, enables the analyses and recommendation arrived at, in this study, to generate a child-friendly set of remedies that will, reduce and eventually eradicated, the risk and harms faced by children, through the lens of, for example, a child's best interest and evolving capacities in South Africa. The desk-based research mainly enables the collection and analyses of existing literature on the right to digital safety for children in South Africa. The primary sources consulted is relevant legislative instruments in South Africa, including, but not limited to, the 1996 Constitution, the POPI Act (POPIA), the Cybercrimes Act, and other relevant legal instruments extant in South Africa. This study, also consults the African Children's Charter and the UNCRC, given South Africa's ascension to these instruments.

The secondary sources that have been consulted are journal articles, books, government and other relevant reports.

7. Limitation of the study

The major limitation in this research is the decision to not have a qualitative aspect. A central argument I adhere to in this research, is that of including and involving children in decision and suggestion making. Yet, in my study I will not have the direct voice of children. This is done because for two primary reasons: firstly, lack of adequate training to carry out field study; and secondly because the study is a policy level investigation. It would have been ideal to include the voice of children to offer policy reforms. However, because I do not have adequate training to collect raw data from

children, it would be amiss to be exhibit such enthusiasm. Furthermore, I would not be able to adequately use the data collected. In overcoming this limitation, I will look to available research from other scholars especially any reports and studies that include the voices and opinions of children.

8. Structure

This mini-dissertation is comprised of 4 chapters. It begins with an introduction that sets the positioning of the study and flows into chapter 2 which ascertains the South African context of the problem. In this chapter, the dissertation evaluates the sufficiency of South African domestic laws that protect children's digital rights. In the third chapter, the study identifies the harms that are faced in the digital sphere, and contextualises them using regional best practises as a bench mark. In the fourth and final chapter, I will offer recommendations that would, possibly, bridge the gap between the exposure to harm that is proliferated by rapid technological advancements and the enactment of requisite protective laws and policies.

Chapter 2: Defining Digital insecurities

1. Introduction

In a world rife with multiple cybercrimes and reinventions of harm, it is considerably untenable to say that there is imminent harm if it cannot be described. It is therefore necessary to define the harm for it to amount to a crime or insecurity. If indeed one can allege merely opening a device can expose them to a number of insecurities, then the nature of the exposure must be capable of definition. This is also important because the premise of proactive protection requires adopting principles such as safety by design.[36] This principle calls on understanding the harm and exposure factors so as to design relevant and applicable legislation or policies for regulation.

This chapter first discusses the bedrock of cyber interactions, which is personal information or data. Understanding what role personal data plays in creating vulnerability lays a foundation for the discussions that flows through the subsequent chapters of this mini-dissertation. At the heart of the discussion of evaluating cyber security of children two things are important: understanding the value of data and how to protect it; and secondly understanding cybercrime to correctly protect against it. One of the key components that is violated is personal information and thus the need to have an appreciation for what it is and its position in the greater discussion.

This chapter seeks to look at the forms of internet insecurity that are used to manipulate personal information. By so doing, it explores the relationship between personal data and cybercrimes. The list of cybercrimes, like crimes in general, is long. In order to contain the current discussion and evaluation, the discussion is limited to phishing; data mining; and algorithmic manipulation. These three are chosen primarily for their interrelated nature and how they are often at the centre of cybercrimes that relate to children.[37]

[36] World Economic Forum 'Safety by design (sbd)' n.d. https://www.weforum.org/projects/safety-by-design-sbd (accessed 10 October 2023).
[37] Kaspersky 'Internet Safety for Kids: How to Protect Your Child from the Top 7 Dangers They Face Online' n.d. https://usa.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online (accessed 10 October 2023).

2. Personal Data

Personal Data or interchangeably referred to as personal information is self-explanatory. It is data or information relating to an individual.[38] This can be information ranging from the name of a person to other identifying factors such as their date of birth, identity numbers, and any other habits or identifiers. The value of information in the age of the internet of things has risen significantly.[39] Data holds significant value. It allows the holder to broker deals, to gain political leverage, and even have financial gain.[40] What all these have in common is that they are information fed machines. And in a similar manner the internet is not a self-sustaining machine independent of individuals, it requires data to grow and give back information that is valuable. However, information can only be valuable in so far as it is relevant. As such, there has been a noticeable increase in the trading of personal data that is acquired and stored with greater intent of understanding the persons it belongs to and represents. This has created more reliable information and relevant products. The internet of things, though a complicated exchange of information, has undoubtably given back value for the trade-off.

In the pre-Covid era, personal information found or shared through the internet was scalable and easier to follow because there was a hybrid of physical and online activities.[41] And even in the hybrid format that existed, the interactions that were valuable were mostly done in person and online interactions were not depended on as being vital to transactions and services. However, because of the implementation of measures limiting physical movement during the Covid pandemic, many work systems and personal activities had to be moved to online systems. Thus, we experienced a large scale and quick shift in the increase of online presence and the sharing of information online.[42]

[38] DA Hoffman & PA Rimo "It takes data to protect data" (2018) *The Cambridge Handbook of Consumer Privacy* 546.
[39] n38 above, 550.
[40] Jurcys P 'What is the value of your data' 6 September 2019 https://towardsdatascience.com/what-is-the-value-of-your-data-9341cd019b4d (accessed 10 October 2023).
[41] Campbell-Kelly M & Garcia-Swartz DD 'The history of the internet: the missing narratives' (2013) 28 *Journal of Information Technology* 18-33.
[42] Interpol, 2022 Interpol Global Crime Trend Summary Report.

The aim of the expansion through social media and other internet services was to create a global community. This was even reflective in Millennial Development Goal 8 (MDG) resolved by the UN in an effort to create better international relations. Similarly in Sustainable Development Goal 17 (SDG), there is a call to "strengthen the means of implementation and revitalize the global partnership for sustainable development" And so, the problem has not been in the result of a globally connected world, but the timing and modes of connection which have found organisations and stakeholders unprepared for the change and with no sufficient security systems in place.[43] Internet Service Providers were found handling significantly more personal data, in the forms that were different and nuanced more towards specific retail value. This will be further explored in the section detailing the selected cybercrimes.

An important aspect of connection and mutual development is sharing and using personal data. As such, it is important to understand the value of personal data in the age of interaction through the internet of things. Personal data is a lucrative commodity. It provides insight into a person, and a person is a representation of a fraction of any human consumer market, which in essence is every market. The person and their values shape various markets[44]. Therefore, to understand any market and ultimately make a profit from it, it is important to collect data about the people that make the market. Since data plays the role of insight into markets and possible trends and profit lines, it has been hailed the diamond or oil of our age.[45]

Companies are investing in personal data. It is reported that up to billions in dollars are spent to acquire this data from third party collectors of data, meaning data collected by X of Y.[46] How and what companies acquire is affected by numerous variables such as demographics, personal identity details, family status, finances, and individual hobbies and activities.[47] With the global price of data ranging from as low as USD$0.0005 to as much at USD$2, companies, especially tech giants such as Meta,

[43] SERR Synergy (n8 above).

[44] Jurcys (n40 above).

[45] Jurcys (n40 above).
[46] As above.
[47] As above.

are profiting from the economics of numbers.[48] And so, when speaking of the value of protecting personal data and effecting cyber security, the call is also to ensure that people are not being exploited for profit without their knowledge. In order to put this into perspective, between May and July of 2017, a credit reporting agency Equifax was the "victim" of a cyber breach resulting in hundreds of millions of Americans, British and Canadian nationals having their information compromised.[49] Working with the numbers discussed above, the nature of information stolen would have weighed more expensive and resulted in a healthy profit margin for the hackers.[50]

Data is targeted because it is easy to access due to often poor security measures, and low investment into cybersecurity measures. The common rhetoric about data safety is said to be strong passwords and different passwords for various accounts. However, research shows that the threats posed by cyber criminals actually go beyond first party protection.[51] The breach is often done to the third party companies having their system compromised, which then leaves persons vulnerable.[52] As Maras puts it, the individual victims cannot shield themselves from the risk posed by the vulnerability of third parties that are storing the data and having it stolen from their servers.[53] In the following sections we look at the different forms of breach carried out by cyber criminals.

3. Phishing

In the simplest form, phishing is trickery intended to either introduce malware, have an individual unknowingly share personal information or introduce a weakness that exposes their system and or organization to cybercrime.[54] Phishing is a common form

[48] As above. See also L Bershidsky 'Let users sell their data to Facebook' 31 January 2019 https://www.bloomberg.com/view/articles/2019-01-31/facebook-users-should-be-free-to-sell-their-personal-data?leadSource=uverify%20wall ("accessed 10 October 2023).
[49] AN Novak & M Olguta Vilceanu '"The internet is not pleased": twitter and the 2017 Equifax data breach,' (2019) 22:3 *The Communication Review* 196-221.
[50] As above, 196.
[51] United Nations Office on Drugs and Crime 'Cybercrime that compromises privacy' https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-10/key-issues/cybercrime-that-compromises-privacy.html (accessed 11 October 2023).
[52] As above.
[53] M Maras 'The Internet of Things: Security and Privacy Implications' (2015) 5(2) *International Data Privacy Law* 99-104.
[54] IBM 'What is phishing?' n.d. https://www.ibm.com/topics/phishing#:~:text=Phishing%20is%20the%20most%20common,and%20pr

of malicious social engineering that relies on deceiving, pressuring and manipulating persons into sending information to the wrong people.[55] Common examples of phishing are emails of persons masquerading as long lost relations offering an inheritance; or persons posing as an institution a bank or other service that may have access to personal information, and they will claim to have an error that requires sharing of personal information to rectify the error.

Children today are considered to be more tech savvy. As a result, they have a confidence bias when it comes to their internet susceptibility, in that they are more likely to think of themselves as knowing more than not. Most children are reported to be aware of what constitutes phishing, and the need to guard against sharing personal information, but yet still part with personal information.[56] Kaspersky, a global tech company through its threat intelligence experts carried out research into the safety of children online and evaluate what children understand about cybercrime, especially phishing.[57] This research found that 2 out of 5 surveyed children who believed themselves to be knowledgeable about phishing, were in fact victims of phishing.[58] The research also found that adults in these children's lives were not assisting or teaching their children about cyber safety and more often, assumed they knew how to keep safe in digital space.[59] This all brings to attention the need for the understanding of the risk that is carried with cybercrime. Part of the adults in these children's lives believing that they could take care of themselves can be contributed to the tendency to think the threat is far removed from them and not worth investment of time and energy. Understanding the scope of risk and implementing policy to combat and mitigate these risks will not only protect the rights to safety of the children but also limit the form of harm they are susceptible to.

4. Data mining

Data mining is the process of uncovering patterns and other valuable information from large data sets, or collections of data.[60] It relays on high-quality data and effective

essure%20tactics%20for%20success (accessed 10 October 2023).
[55] As above.
[56] Kaspersky report, Overconfident and over exposed: Are Children Safe Online?
[57] As above, 6.
[58] As above, 6.
[59] As above, 7.
[60] U Viswanathan 'Data mining: Helpful or harmful? Exploring the benefits and dangers of big data' 26

information sharing.[61] Data mining on its own is not a crime nor is it wrong. It is a legal form of knowledge creation that used by some industries to improve output. However, much like any other useful practise it is dangerous when put in the wrong hands. Negative data mining can result in privacy invasion, cyberbullying and harassment, identity theft and many other insecurities.[62] Children whose privacy is invaded can have key personal information about them and others around them exposed and have their lives upended. A more devasting outcome would be that of identity theft. A child whose identity is stolen at a young age is likely to only understand the full effect of the crime committed against them much later in their lives.[63]

A known example of the outcome of negative data mining is that of the Facebook and Cambridge Analytica scandal. News of privacy breach by the two companies travelled all over the world in March of 2018.[64] Cambridge Analytica, a data analytics company created "pyscho-graphically tailored" advertisements by collecting the personal data of 87 million Facebook users.[65] The intention of the "product" was to influence the voter's preference in the 2016 US Presidential elections. When this information became public after an employee reported on what was being done there was wide spread concern and dissatisfaction with the manner in which private information was being used.

For the first time at a global scale, the value of traded private information became topical. The conversation surrounding the power that large, big data companies have when they handle and store persons personal information had to become a real social issue and not just an academic conversation. The conversation transcended beyond people being bombarded through many advertisements, to people have advertisements being tailored to their proven biases so as to influence human nature. In this instance it was influence towards the selection of a world leader, whose policies

May 2022 https://www.mcgill.ca/cybersafe/article/data-mining-helpful-or-harmful (accesses 17 October 2023).

[61] As above.

[62] Xu et al "Information Security in Big Data: Privacy and data mining" (2014) 2 *IEEE Access* 1-28.

[63] As above. See also Berman, et al 'Children and the Data Cycle: Rights and Ethics in a Big Data World' (2017) https://www.unicef-irc.org/publications/907/ .

[64] J Hinds et al '"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal' (2020) 143 *International Journal of Human-Computer Studies* 1-14.

[65] As above.

can affect global activities and trajectories. This poses a risk of violation of human dignity at its core. The same transposed to the lives of children is a danger that will outlive its creator. Beyond the risk posed in exposure today, children are tomorrow's world society, and harm or violation of the foundations of their social fabric is a destruction of a future, and a violation of very real human rights.

5. Algorithmic manipulation

Closely related to the scandal that unfolded with the Facebook and Cambridge Analytica scandal is algorithmic manipulation (AM) which is rampant in social media use. This concern is rife in the conversation concerning the safety of children online. The concern surrounding this phenomenon of AM has been exacerbated by the increased use of social media and noted trends with social media use and social deterioration.

There is no strict definition of the phenomenon as it is named after its function. Algorithmic manipulation is the influencing of behaviour that arises from a study of a person's online habits and predicts other biases and tendencies that will otherwise keep a person using a platform. Some authors argue that it is a key back bone of personalization systems and gatekeeping roles that social media has developed in recent times.[66] At the heart of the practise is an intention to "overtly persuade—and covertly manipulate—users for the sake of engagement."[67] This in the context of children's interaction online poses an imminent threat. A threat to their autonomy but also a threat to their development. Child development has been, time and again proven to be shaped by what they are exposed to in their surroundings, and the possibility of one siding the exposure and more so to dangerous material, will hamper their development negatively.

AM poses various forms of harm. It can lead to self-harm, substance abuse, polarization, radicalization amongst other forms of harm. At the core of these outcomes is no singular cybercrime, however the process leading to them must be considered to be a cybercrime and dealt with in such a manner through policy and

[66] U Reviglio & C Agosti 'Thinking outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media' (2020) 6(2) *Social Media + Society, Sage Journals* 1-12.
[67] Reviglio & Agosti (n66 above) 3.

legal reforms that contain how personal information can be used. It is arguable that if it can be proven that exposure to X can lead to behaviour that is detrimental for society that violates fundamental rights and securities, then the same must be outlawed. Alter describes social media, as a single example of the internet being "addictive by design."[68] He argues that there is a move to satisfy the individual economy that produces misinformation as a by-product of the need to make what is appealing to the individual. This is only a small fraction of the argument of how AM is causing the internet and the information it produces to be harmful.

A controversial example of this form of cyber insecurity is the presence of AM during the use of Tik Tok by children. Writing in a 2022 report on the harm for children of Tik Tok Algorithms, Imran Ahmed of the Centre for Countering Digital Hate, writes that "[t]he algorithm recognises vulnerability and, instead of seeing it as something it should be careful around, it sees it as a potential point of addiction."[69] The report details how the social media application has allowed children under the age of 13 access to it and has not acted in a manner to protect their participation and consumption of information on the platform.[70] This is in light of the platform purporting to not allow users under 13. The only security measure in place to evaluate this is the child stating that they are 13. What is more, the platform is driven by the constant and recurring use. As such when it is described that it views vulnerabilities as being an opportunity for addiction, it is a move to increase the tendency of users staying online and increasing revenue for the platform. This is at the cost of the mental health and security of the users, in this case, children. Beyond their access to harmful content and psychosocial manipulation there is also the vulnerability of their information which is now accessible for further harms from cyber criminals.

6. Conclusion

The contents of this chapter unpack the harms faced by persons interacting online, but at the core how the harm affects children. The intention of this chapter was to expose the nature of the problem, its components, and how they can be perceived by

[68] A Alter *Irresistible: The rise of addictive technology and the business of keeping us hooked* (2017).
[69] Center for Countering Digital Hate, Deadly by Design. TikTok pushes harmful content promoting eating disorders and self-harm into users' feeds.
[70] Same as above.

a State in order to provide adequate protection through policy and legislative implementations. The following chapter evaluates the legislative position of South Africa on children's safety in the digital space and will be positioned at addressing the harms that are specific to the nature of cyber interactions as unpacked in this chapter.

Chapter 3: South Africa's existing legislative framework related to protecting children's interaction with the digital space.

1. Introduction

In March of 2022, the government of South Africa through the Government Communication and Information System (GCIS), urged children to become active digital citizens and to take full advantage of their digital rights.[71] During a webinar hosted by the GCIS on 29 March 2022, stakeholders acknowledged the importance of the participation of children online, and alongside this participation the need for the education of online safety.[72] The various stakeholders acknowledged the duty and place of the state in educating the safety tools and practices online, which all align with the duties placed on the state through its international obligations.

The provisions of child protection in the UNCRC and the African Children's Charter places an obligation on states parties to action digital safety.[73] In addition to this, an important aspect is to do so within a Children's Rights Based Approach(CRBA), which some may argue is simply a Human Rights Based Approach (HRBA) that focusses on the rights of the child.[74] The tenets of the approach seek that service delivery, or in this case policy, is formulated in a way that aims at centering the needs of the rights holder.[75] Using the conceptual and methodological framework of the OHCHR, an evaluation for structure, process and outcome will give insight into how the steps taken by a state have performed in meeting their obligations.[76] The OHCHR puts it this way,

[71] https://www.sanews.gov.za/south-africa/children-urged-take-full-advantage-their-digital-rights
[72] As above. Some of these stakeholders included Representatives from The Film and Publication Board and Media Monitoring Africa, as well as learners, educators and parents who were the primary recipients of the information that was to be shared.
[73] See article 10 of the African Children's Charter and article 16 of the UNCRC.
[74] A founding discussion of understanding the tenets of CRBA and how it relates to HRBA is give in the work of Kišūnaitė, Aida, and Ly Hai Bui. "Operationalising children's rights principles: an indicator framework for policy analysis." (2021) *Revista sobre la infancia y la adolescencia* 20:1-21.
[75] Same as above, 4. See also https://connect.scot/news/connects-summary-taking-childrens-human-rights-approach-guidance.
[76] Main features of OHCHR conceptual and methodological framework

the assessment will evaluate " commitments and acceptance of international human rights standards (*structural* indicators), to efforts being made to meet the obligations that flow from the standards (*process* indicators), and on to the results of those efforts (*outcome* indicators)." Looking at the following pieces of Legislation through this lens, but specifically that of the principle of the best interest of the child,[77] amongst other relevant rights in the digital environment,[78] will drive the discussion in a direction that will allow an evaluation of state efforts against a legal and policy framework centred on child rights, as opposed to a generalist approach.

Since, South Africa's ratification of the UNCRC on 16 June 1995,[79] and the African Children's Charter on the 7 January 2000,[80] the State has not enacted national laws with a specific aim to provide digital security for children. The two pieces of international law are silent on cybercrimes against children, but mainly as a result of when they were drafted. However, there has been legislation that protects the general citizenry of South Africa, and by extension there is protection for children. The most recent of these is the Protection of Personal Information Act (POPIA), [81] making it a culmination of the State's efforts to ensure digital safety for both children and adults.

This chapter provides an analysis of the scope and objectives of the relevant legal instruments applicable in South Africa. It evaluates the extent to which digital safety has been envisioned by the legislator, and how the enacted laws interact and combat digital insecurities. This analysis will be carried out by looking at relevant legislation and academic commentary. Following this, this chapter will discuss the obligation that exists for South Africa as a State party to the UNCRC and the African Children's Charter. Indeed, leading into this conversation there is a need to also have an appreciation of the holistic South African legal system and its jurisprudence.

Human rights indicators see: https://www.ohchr.org/en/instruments-and-mechanisms/human-rights-indicators/main-features-ohchr-conceptual-and-methodological-framework

[77] Article 3 of the UNCRC.

[78] These are the rights that are broadly encapsulated in the discussion of this mini dissertation, such as the right to privacy and the right to information, amongst other unmentioned rights.

[79] Ratification status of South Africa, available https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=162&Lang=EN

[80] Ratification status to the ACRWC, available https://au.int/sites/default/files/treaties/36804-sl-AFRICAN_CHARTER_ON_THE_RIGHTS_AND_WELFARE_OF_THE_CHILD.pdf

[81] Protection of personal information Act 4 of 2013, herein after, POPIA.

The South African legal system hails from a mixed legal history.[82] In its colonial foundations it is dualistic in that it has roots in the Roman Dutch Law, which came with the Dutch settlers and the English Common Law system. These two along with the customary laws of the native people, have been transformed and developed to create what we perceive as South African Common Law and the codified Roman Dutch law.[83] Prior to the enactment of any piece of relevant legislation,[84] common law was the only existing form of protection or redress for digital harms.[85] Common law provided (and continues to do so today), punitive recourse for forms of cyber-crime, that can be argued and made to comply with the tenets of common law crimes.Examples of criminal law crimes that could be used to connect to cybercrime include extortion, *crimen iniuria*, defamation and assault. Snyman defines *crimen iniuria* as the unlawful intentional and serious violation of the dignity or privacy of another person.[86] This form of protection though important in ensuring there is base level protection, has many hurdles when trying to provide full and complete protection against cybercrime. As such, the legislator in creating specific laws that address cybercrimes, helped to broaden the scope of protection available for children under South African law.

In the following sections of this chapter, the focus turns to specific pieces of legislation, in their order of enactment. It looks at how they offer protection for the South African, and if it specifically protects children as a different people group. There is a discussion of the short comings or portions that the legislator is otherwise silent on that may be of importance to broaden the protection of the legislation. The first of these is a discussion on the first piece of legislation South Africa enacted with the aim to ensure digital safety.

---

[82] AJ van der Walt 'Legal history, legal culture and transformation in a constitutional democracy' (2006) 12:1 *Fundamina: a Journal of legal History* 1-47.

[83] Same as above, 4.

[84] This is to say any legislation that is specific to the subject matter, cyber insecurity.
[85] I would argue it provided punitive measures and not protective measures, and so the word protection is a bit generous. However, for the purpose of this argument it acted retrospectively and did not aim to hinder anything. However, the threats available today are distinctively different to those available in the early 2000s. And so, the two are not comparable.
[86] CR Snyman *Criminal Law* (2008) 469.

2. Electronic Communications and Transactions Act

The Electronic Communications and Transactions Act (ECTA),[87] was enacted in 2002 as a subject specific legislation for the facilitation and regulation of electronic communications.[88] The Act overall deals with regulation of transactions and communications that take place online and sets out the e-strategy for the republic.[89] In chapter 13 of the Act, a broad detailed list of cybercrimes is listed. The list is not exhaustive and does not include child specific cyber harms, for example cyber bullying, cyber grooming, phishing and other like cybercrimes. The formulation of cybercrimes in Chapter 13 of the Act, is general and aimed at being expansive so as to cover multiple crimes. For example, Section 87 of the Act details computer-based extortion, which can find extension and application to crimes such as cyber-bullying.[90] The tenets of extortion as per the Act allow for redress to be sought through a progressive reading of the text. The legislator in so doing misses an important opportunity to be specific to the protection of children and acknowledging that there are electronic transactions that can affect children. Specificity in this case would also have been advantageous because in the same manner that the legislator states that abuse of electronic communications or information systems to degrade, humiliate, harass, or even threaten a person are outlawed; [91] there was room for an explicit outlawing of bullying (as an example) as these are the tenets of cyber-bullying.[92]

ECTA as a protection piece of legislation is designed or intended to provide cyber security through regulation of electronic communication. This communication includes the communication that children are involved in but does not necessarily factor how the vulnerability of an adult will seem different to that of a child. The failure to distinguish between the groups of persons was a short-sighted overview that leaves a legislative lacuna in the protection of the interaction of children online. However, considering the enactment of the Act in 2002, it was probably not a pressing of well

[87] Act 25 of 2002.
[88] Preamble of the ECTA.
[89] This has since developed, as such the e-strategy of the Republic at the time.
[90] ECTA, Section 87.
[91] ECTA sections 86 to 88 when read together can enhance this view and bring together the relevant principles.
[92] S Snail 'Cybercrime in the context of the ECT Act' (2008) 16:2 *Juta's Business Law* 36-69.

discussed area of advancement in law, and this would have seemed as a sufficient form of protection for the group of the population intended to be interacting online.

Although the legislator had the mind to approach multiple forms of cybercrimes and predict them, there are nuanced forms of cyber enabled crimes that were otherwise unaddressed. Malware invasion and other viral based harms do not always incorporate or involve communication between parties. As such, the law enforcement stakeholders would have to consider how to bring in crimes such as voyeurism or commonly known as “peeping toms” of the internet. As mentioned earlier, when the regulation of the use of the internet is designed and approached as an instrument for the use of adult communication,[93] a lot of the nuance dangers adults can evade are not tailored to be prevented for children. Thus, ECTA can provide recourse for the harms that arise during communication online but fails to offer preventative or commonly termed “safety by design” standards for Internet Service Providers and other key stake holders in the digital space.[94] One would expect that this particular piece of legislation would have been couched in a policy framework that not only seeks to remedy the wrongs after commission but also provide guidelines that allow for pre-emptive protection. However, the Cybercrimes Act, discussed below, repeals sections 85, 86, 87, 88 and 90 and does away with the argument of ambiguity in the protection through the broad terminology of the law in the Act. [95]

3. Cybercrimes Act

The legislator has codified the crimes created and regulated by the common law and ECTA, through the enactment of the Cybercrimes Act. The preamble of the Act lays the purpose of the Act as the creation and definition of crimes that have a bearing on cybercrimes, and to prescribe penalties for these crimes, develop improved forms of investigation and adjudication, but most impressively the transnational collaboration with other states.[96]

---

[93] S Miller ‘Child protection in the digital world: Why is it needed?’ 2023 Save the Children, see https://www.savethechildren.net/blog/child-protection-digital-world-why-it-needed#:~:text=The%20fact%20is%20that%20the,relevant%20international%20laws%20%5B1%5D.
[94] Same as above.
[95] The Schedule to the Cybercrime Act.
[96] Preamble of Cybercrimes Act. I believe the attempt by the legislator was to bring together the cybercrimes that were otherwise scattered and harmonise the legislative framework of cybercrime in South Africa. Therefore, the assertion of creation of new cybercrimes is merely the bringing together of

Part A of the Act is divisible into 3 divisions of cybercrime. These are a mixture of previously existing (and codified) crimes and newly codified crimes. The three are divided as follows: i) Cybercrimes in general; ii) Malicious communication crimes; and iii) Offences that are incidental to the commission of cybercrimes. By so doing the legislator has brought together the crimes incidental to interaction within the digital space and the relevant penalties. The legislator corrects the shortcomings of ECTA, and enunciates what cybercrimes are and how to identify them with more specificity.[97]

However, the text of the Act is not loud in its specificity of crimes relating to children. The mention of children is limited to the modification of laws existing concerning child pornography.[98] Although this is a development worthy of praise, it is limited to the singular crime of child pornography and is unfortunately reserved for the amendments and repeals section of the Act.[99] The failure to prioritise the discussion of cybercrimes relating to children is shortcoming on the part of the legislator that leaves room for failure in effecting even the provisions available through the Act. It is not wholly necessary for the legislator to make specific mention of children, but it is beneficial when the legislator pre-empts and guides the approach of relevant stakeholders in the enforcement of the law specific to a significant group of the population.

4. Protection of Personal Information Act

The introduction of POPIA into the data protection conversation was ground shifting for the cyber security space in South Africa. Enacted in 2013, but with important sections only coming into effect in 2021, the Act marked a new dawn in digital safety legislation in South Africa. In Section 2, the scope of the Act is highlighted as being aimed at providing protection and regulation mechanisms for the processing of

crimes that were vaguely created through the jurisprudence of the courts and other pieces of legislation, and in this case specifically the ECTA.

[97] See Part A of the Act.

[98] The schedule in its repealing and modification of offences related to child pornography in varying pieces of legislation.

[99] One may argue that this done to not fix what is not broken in the existing framework of protection for children against sexual exploitation crimes, however, the crimes in the area have been evolving beyond mere pornography. Grooming has seized to be regarded as a gateway crime, but it is becoming a full-fledged practice of its own. Failure to address this leaves open an opportunity that was otherwise ripe for the picking.

personal information and data.[100] In particular, the Act states that its primary aim is to give to persons rights to protect their personal information and data. It also gives the power to assert such rights through the regulation bodies of POPIA as it enacts.[101] Through a reading of the Act beyond its scope clause, one is able to see that although it protects one of the fundamentals of digital interactions, personal data, it is limited in the discussion of protection from digital insecurities as a niche and specific area of insecurity.

Looking at the list of the forms of digital insecurities one may face whilst interacting online, personal data or information is not always a primary tool that is a key component of their exposure to danger or risk. For example, a child whose images are solicited for child pornography will have more than just their personal information being used in the crime. In order to complete this crime, the perpetrator need not know identifying or unique factors of the individual, especially if the crime they are to be held under is the possession of child pornographic material. Under Section 4 of POPIA, this perpetrator would face penalty for unlawful processing of the image. One dealing with such a case would have to unravel the nature of personal data/information and make a case that though not the primary processor of the image, the holder of the image is equally liable as the first to process the information. As can be seen, there is already the issue of extrapolation for protection. Because the Act is broad in its scope, specific cases and ones entailing children will be a matter of weaving together principles.

A similar example in the context of POPIA would be cases of grooming and exposure to predators. A child who with the consent of their parents/guardian signs up for online interaction platforms is exposed to interactions that may be harmful. The interaction will not entail a trade of the child's personal information, or unlawful acquisition of the information. As such, to apply POPIA to this scenario will again prove to be a cumbersome effort that really at the end of the day defeats the notion of developing the law for better protections.

Although these loopholes exist, POPIA does present some digital safety for children. Children's information is regulated as to how and when it may be processed. And like

[100] Section 2, POPIA.
[101] Section 3 of POPIA highlights the rights of the individual.

every other individual in South Africa, the children have the option to request that their personal information be deleted or used in specific ways.[102] However, children can only use this power through a third party who is either their parent or a guardian.[103] These persons often act within the best interest of the child, or at least they are presumed to be acting in this manner. However, in order for this to truly adhere to the best interest principle, then the child should be given room for autonomy. What does autonomy look like? Though there are varying studies surrounding maturity and age, it is also a child's right to have primary autonomy over their information and enforcing any rights they desire to enforce with regards such information. If a child, for example at age 15, has to wait for their parent to enforce their right on their behalf, there is arguably a failing of the child's interests.

Digital safety as discussed in chapter 1, looks at cyber bullying, child sexual abuse; identity theft; phishing; predator exposure and many more forms of danger.[104] As such, the discussion of relevant means of protection herein must cover to as far an extent as is possible, the varying forms of digital safety. What is more, these protections must hold to standard of the best interest of the child. This is because the aim of establishing the level of protection available must be able to be as child centred as possible. The exposure children face online is different to that of adults.[105] Subsequently, the child centred dynamic must be brought into the purview of child protection.[106] What is evident with the laws discussed in this chapter is that although there is effort, it amounts to refurbishment of the same wheel that is not all encompassing. There are laws but the adequacy of these laws is lacking.

[102] Section 4 of POPIA.
[103] This is primarily because of the limited legal personality that children have in South African Law.
[104] The list for what may constitute cybercrimes or digital insecurities is not exhaustive. For the purpose of further reading, there has been attempts at ranking the types of dangers and the statistical exposure thereto. See https://usa.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online
[105] In supporting this lane of thinking, Cassim posits that internet was not made for children, but was rather made for adults. As such the dangers are primarily made to be tackled by adults. See F Cassim 'Formulating adequate legislation to address cyber-bullying : Has the law kept pace with advancing technology?' (2013) 26 *South African Journal of Criminal Justice* 1. See also Miller in n87 above.
[106] This is also important especially when considering that the best interest of the child is a constitutional principle, and as such of high value in being upheld. See Section 28 of the South African Constitution.

Looking at these pieces of legislation in the methodological and conceptual framework of the OHCHR as mentioned earlier, the following can be deduced: firstly, there are structural indicators, and they adequately examine the legal lacunas, but there is no specific awareness of the obligations arising from internal law or treaty obligations. The second component which is the process indicators, is aimed at evaluating the sufficiency of the implementation tools: there are no legislated implementation tools that are focused on implementation of the protection of the rights of the child. The State shows effort to have round table discussions that will empower such implementation but does not follow through by legislating or in the least creating policy frameworks that support the implementation of the obligation fulfilment. Lastly, concerning the outcome indicators: although there is not a lot of research on the impact, it can be argued that the lack of focus on the specific rights and obligations towards the holders is likely to present loopholes in evaluating outcomes. The protection norms given by these pieces of legislation are too broad to be narrowed down to nominable outcomes in the context of children. Thus, though a right step towards creating structures that may be implemented, the outcomes are likely to fall through.

In the coming chapter, thew discussion will turn to the international obligations that South Africa has. In discussing these the aim will be to unpack what South Africa has managed to achieve and where there is room for improvement. In identifying the opportunities for improvement available, this mini dissertation will unpack possible avenues of improvement and add to the growing Knowledge systems contributing to the growth of South African protective mechanisms for children in digital space.

Chapter 4: Recommendations and Conclusions

1. Introduction

Having unpacked the law of South Africa and the standard of protection required on a technical level, it is apparent that there are gaps in need of breaching in order to bring the protection standard of the state up to par with true protection. In order to adequately quantify true protection, understanding the harm is important. This has been done in chapter 2 and a scope of harm has been defined. Another avenue to arrive at defining a form of true protection would defining the obligation existing on the state to protect. What that obligation means and carries and how it can be met will allow a fair evaluation of the protection of the South African laws for children's digital privacy as envisaged in this mini dissertation. As noted, and stressed through the narration of this mini dissertation is the vast nature of the harm as well as its fast-paced change nature, thus ultimately a multidisciplinary approach is a most viable option towards change.

Therefore, in this chapter, the narration begins with unpacking the obligations that exist on South Africa from their international agreements, understanding how they have been met and may not have been met, and ultimately raising recommendations for improvement that flow from these standards of best practise. Following this, the chapter narrates through a multi-disciplinary lens approaches that are available from the discipline of Information Technology that is the encompassing field that the law seeks to relevantly regulate. The aim in offering these recommendations is to show the bridge available between the law and other disciplines, that will bring together true protection for children in the digital environment.

2. Perceiving the problem with a multidisciplinary lens

Public International law, in particular treaty law, states that a state has an obligation to act as per the obligations set out in a treaty they have acceded to.[107] South Africa is a dual system nation and requires that there is both accession and ratification in order to be bound to a treaty.[108] As such through these requirements, the treaties in question

[107] Article 11 of the Vienna Convention on the Law of Treaties.
[108] Section 231 of the Constitution of the Republic South Africa. See also G Ferreira & A Ferreira-Snyman "The incorporation of public international law into municipal law and regional law against the background of the dichotomy between monism and dualism" (2014) 17 *Potchefstroom Electronic Law*

find binding obligation on South Africa. What is more, some treaties ascend into the realm of Customary International Law (CIL) through state practise and *opinio juris*.[109] What is important in this discussion is the binding nature that the principles of the treaty that ascend to CIL. South Africa is a state party to the UNCRC and the African Children's Charter and have obligations in terms of these treaties. However, as of the writing of this mini dissertation, South Africa has only signed the African Union Convention on cyber security and personal data protection (Malabo Convention). This therefore means that the obligations contained therein are not yet legally enforceable against the state.

Two out of the three mentioned treaties do not mention or place direct obligations with regards to cyber security. Therefore, the discussion focusses mainly on the general obligations that are placed on states. This is why it is also important to note that some of the treaty obligations have the nature of principles or obligations of CIL. This therefore binds South Africa to act according to them both in meeting their treaty obligations but also as a subject of public international law. What is more, the system of review mechanisms and general comments allows the literature of the charters to be developed and the obligations that were otherwise not apparent in the black lettering of the text, to be more apparent. This is even more so important as general comments are developed through other peer review mechanisms that take into consideration state practises.

General comments do not create obligations for states. However, they are often used with great authority for the purpose of developing the framework of implementation a state can use. General comments are often developed by committees through their cumulative recommendations offered to states in reports and other review mechanisms. The committees in noting particular patterns and repeated approaches by states will often develop thematic guidelines. These guidelines encased in general

Journal (PELJ)

[109] Jurisdictional Immunities of the State Germany v Italy: Greece intervening, Judgment, (2012) ICJ Reports 99

comments help to better understand and contextualise the obligation or contents thereof that must be placed on states.

The UN Committee on the Rights of the Child in its general comment 25, on children's rights in relation to the digital environment develops the obligations of the state that flow from the UNCRC with regards digital safety of the child. Citing that those children consulted for the purpose of the comment, the Committee highlights that it is not only perceived to be important for children to have access to digital spaces, but by their own admission they find digital technologies to be vital to their lives and future.[110] The committee centralises particular principles in order to evaluate best practises that should be taken by states.[111] It acknowledges that states must effect relevant and up to date laws that can tackle relevant current technological issues.[112] An important contribution that the committee makes in paragraph 24 concerns the implementation of industry codes, design standards and action plans that are aimed at the provision of a digital environment that protects children's rights. Arguably the obligation on the part of the state it to enact legislation that is regulatory of the design standards of corporations handling digital environment markets. At best South Africa has one piece of legislation that meets this standard, POPIA. However, as discussed above, POPIA is not designed to interfere in the actual components that affect vulnerability of children. This therefore leaves South Africa lagging behind on the call to implementing relevant measures.

In a similar format of wording the African Children's Charter manages to offer a more direct right to children. In article 10, the Charter gives children the right to privacy of communications. This right as worded in the charter is silent on the digital environment.[113] Given the time at which it was drafted, this is a reasonable silence, taking into cognisance the era of digital presence as we know today being far ahead

[110] UNCRC General comment 25, n23 above, introduction.
[111] These principles are mentioned in the introduction to this mini dissertation. however, for the purpose of context, these are i) non-discrimination; ii) best interests of the child; iii) right to life, survival and development; and iv) respect for the views of the child.
[112]UNCRC General Comment 25, n23 above, paras 22 & 23.
[113] Article 10 of the African Children's charter verbatims states the following: "No child shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to the attacks upon his honor or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks."

of the time of the drafting of the Charter. However, scholars have argued that it can find application by extension to the digital environment.[114] At the heart of honouring the tenets of this right to privacy is the issue of personal information. The charter covers unlawful arbitrary interference of privacy. The wording of POPIA is aimed at protecting personal information in so far as its handling, its storage, its use, and ultimately unlawful interference. The South African legal regime in this way meets the standard of protection envisioned by the Charter.

The African Committee of Experts on the Rights and Welfare of the Child (ACERW) has also produced commentary work designed to help to better expand of the contents of the charter as is the work of the UNCRC. In their general comment number 5 dealing with state party obligations, expands the standard of obligation a State has to implementing the charter.[115] The Committee describes the intention of the comment as being an unpacking of the obligation of implementation, which they describe as being embedded in all human rights laws.[116] an important aspect of implementation that the committee notes beyond legal and policy measures is budgetary measures that should be taken to aid in effecting realisation of children's rights.

Budgetary measures are important because they create resources for implementation. The economic circumstances of a state differ from state to state, and even within a state the inequalities will differ. What a strategic budgetary measure allows, is for a state to allocate resources as per the growing concerns and needs of a people group. To bring this into the context of South Africa, as discussed earlier in the mini dissertation, education and lack thereof is a leading contributing factor to the implementation of safety strategies. Without the education of safe digital and internet use for learners, there will be a perpetual cycle of vulnerability that is not addressed in time to prevent harm. The education of other stakeholders such as guardians, parents, and educators also equip communal protection mechanisms. What the Kaspersky study cited above shows is that there is vague knowledge by adults who are otherwise

[114] O Masocha Sibanda 'Towards a more effective and coordinated response by the African Union on children's privacy online in Africa' (2022) *African Human Rights Yearbook* 172.
[115] ACERWC General Comment 5 (2018) on "State Party Obligations under the African Charter on the Rights and Welfare of the Child (Article 1) and systems strengthening for child protection.
[116] ACERWC General Comment 5, n109 above, para 9.

in a position to help children avoid harm.[117] Educating and bringing awareness in these spheres of guardianship will assist the state to further their goals beyond the black letter law.

Education is but only one area where a budgetary adjustment approach can have a positive and goal furthering impact on digital security. Allowing budgetary allocation in the development of cyber security technology is also important. In the advent era of predictive AI and rapidly developing cyber harms, maintaining software knowledge that is easily outpaced, it in of itself a digital insecurity. The state needs to invest in the latest cyber security technology as well as understanding the latest cyber insecurity, this allows the production of safety measures that will actually be timely and relevant. This would require an investment in multiple sectors of the government. Firstly education, for the purposes of equipping and teaching persons the information. Secondly, under economic development budget line, there would be need to invest in the innovation, science and technology budget line. As of the writing of this mini dissertation, the 2023/24 budget expenditure is set for R293.7 billion for basic education and R19.8billion for innovation, science and technology.[118] The difference in the two numbers is significant and, in some ways, telling. Although National treasury has a significant amount allocated to basic education, the background context must be considered to see if this can and will trickle down to imagined effects. There is a large literacy problem in the country as a whole with the 2021 Progress in International reading Literacy Study showing that 80% of grade 4 learners could not read for meaning at the same level as their peers across the world.[119] What this study brings to light is the hierocracy of needs and what will receive more budgetary concern for the government. Although it would be noble to prioritise digital security education, some fundamental or elementary issues are still yet to receive attention.

[117] Kaspersky report, n56 above.
[118] National treasury, Budget 2023 Highlights. Available https://www.treasury.gov.za/documents/national%20budget/2023/sars/Budget%202023%20Highlights.pdf
[119] Ten-year study shows South African school reading literacy is slow to improve, University of Pretoria, Available: https://www.up.ac.za/research-matters/article/2801832/ten-year-study-shows-south-african-school-reading-literacy-is-slow-to-improve

The budget allows implementation, however, without policy perception of the problem there will not be a strategy to implement with the available budget. The importance of policy regulation cannot be overstated. Beyond statutory obligations and other legally binding notions of ensuring the state acts in the best interest of the child, there is need for the state to show a policy framework that is purposive to achieve progressive realisation. Without a policy directive, the state remains at a loss for mechanisms that will achieve digital securities for children. In the most recently published digital security draft policies,[120] the document offers expansive guidelines that can assist organisations and companies alike to streamline their policies to achieve the best information security policies. The document is said to be developed through consultation and research of the global best practise trends in the same arena.[121] However, in all 495 pages, children are mentioned twice as a passing remark and again at shallow level engagement.[122] The trend as seen in earlier discussion in the mini dissertation, children are not yet a key area of focus in the digital security conversation. Their insecurity continues to be discussed as a by-product of the danger as a whole and not as a targeted group. The only instances that children are addressed continues to be limited to child sexual abuse materials. This is and will continue to be an area of high significance. But the negation of other forms of insecurities leaves dire consequences unaccounted for and thus children insecure.

3. Conclusion

Ultimately this mini dissertation sought to look at the state of digital security laws and policy in South Africa. Understanding how they are layed out in the framework of leading digital insecurities, and ultimately how they are being contextualised for children. The following key issues were found: the lack of child specific legislation and policy; a surface level approach to prevention of harm; intersectionality of the digital security problem with other socio-economic issues, thereby limiting the capacity to address. In order to contextualise these findings, this section of the mini dissertation will conclude on the issues through the answering of the research questions posed and positioning the multidisciplinary solutions available.

[120] Draft policies information security policies available: https://www.gov.za/sites/default/files/gcis_document/201409/infosecure0.pdf
[121] As above, 2.
[122] As above, 413 & 456.

The first question that the mini dissertation sought to uncover concerns the harms faced by children online in the South African context that call for more specific forms of protection? As found through the research herein, the harms faced by children transcend the commonly recognised child sexual abuse material. There is harm that will impact on their social security through identity theft, personal information abuse and similar harm. Children are also at a higher risk of psychological and social manipulation through targeted manipulation by predative social media companies and other online services. What was more apparent is that the approach has been negating the individuality and specificity of children's cases.

The second question that the mini dissertation sought to cover is how has South Africa addressed children's digital safety? Unfortunately, beyond the mentioning of children in passing or in very brief sections of the available legislation, there was a general failure to have child centred legislation, policy or any high-level strategic plans. South Africa is not silent to the digital harms nor the need to aid children in their interaction with digital spaces. However, South Africa is seemingly slow to come to the table to create specific solutions for children.

The third area of inquiry that was a key output area is how beyond the black letter law, how can strategic litigation and advocacy aid in creating effective law and protection? The international obligations and suggestions of the relevant committees (UNCRC and ACERWC), have all pointed towards the need for correct conceptualization of the matter. Beyond the black letter law, the incorporation of digital security in the fabrics of what will improve economic output and country development is a key framework change. Ultimately the prioritisation of implementation is also important beyond creating the new laws. Budgetary adjustments and realignments, as well as policy reframing will not only create better black letter law, but also create better output of the black letter laws that the State puts into place.

Finally, to address the main research question of how the law can be made more effective as a tool for ensuring child online safety in South Africa, the answer lies in the multidisciplinary approaches available to the state. There is need for understanding the cross-sectional issues that affect the challenge of creating robust digital security measures for children. In unearthing this primary concern, the State will be able to better identify the intersectional areas of issues that will better collaborate to bring out the intended outcome.

Effective digital safety measures for children are not an overnight invention, however they are not impossible to achieve. For South Africa this is within reach and will require decisive turns towards viable solutions. Through the contributions of this mini dissertation, and other scholarly work, there is an array of solutions available for implementation. The cases of cyber bullying that lead to senseless loss of life, can have protection measures that are put in place through the security measures enacted by the state. The same measures will be able to better detect when children's dignity is being compromised and ultimately bring together a more robust protection for the children online in South Africa.

Bibliography

Books

CR Snyman Criminal Law 5ed (2008) LexisNexis: Durban

Case Law

Jurisdictional Immunities of the State Germany v Italy: Greece intervening, Judgment, (2012) ICJ Reports 99

Journal articles

Chynoweth P 'Legal research' in A Knight & L Ruddock (eds) *Advance research methods in the built Environment* (2008)

F Cassim
'Formulating adequate legislation to address cyberbullying: Has the law kept pace with advancing technology?' 2013 *South African Journal of Criminal Justice* 26:1

Livingstone S 'Children's digital rights: a priority.' (2014) 42 *Intermedia* 20-24

Lievens E 'Growing Up with Digital Technologies: How the Precautionary Principle Might Contribute to Addressing Potential Serious Harm to Children's Rights,' (2021) 39:2 *Nordic Journal of Human Rights* 128-145

Stadniczeńko D 'Children's Rights In The Digital Environment Under The Convention on The Rights of The Child' (2022) *Teka Komisji Prawniczej PAN Oddział w Lublinie*, 15:2, 321–331

Rose T 'A human rights-based approach to journalism: Ghana' (2013) *Journal of International Communication* 19(1) 87

S Snail 'Cybercrime in the context of the ECT Act' (2008) 16:2 *Juta's Business Law* 36-69

O Masocha Sibanda 'Towards a more effective and coordinated response by the African Union on children's privacy online in Africa' (2022) *African Human Rights Yearbook* 172

G Ferreira & A Ferreira-Snyman "The incorporation of public international law into municipal law and regional law against the background of the dichotomy between monism and dualism" (2014) 17 *Potchefstroom Electronic Law Journal (PELJ)*

Local Legislation

The Constitution of the Republic of South Africa, 1996

Electronic Communications and Transactions Act 25 of 2002

Protection of Personal Information Act 4 of 2013

The Cybercrime Act 19 of 2020

International Conventions and General Comments

The Vienna Convention on the Law of Treaties.

United Nations Convention on the Rights of the Child Adopted 20 November 1989, entered into force 2 September 1990, 1577 UNTS 3

African Charter on the Rights and Welfare of the Child Adopted 11 July 1990, entered into force 29 November 1999, CAB/LEG/24.9/49 (1990)

ACERWC General Comment 5 (2018) on "State Party Obligations under the African Charter on the Rights and Welfare of the Child (Article 1) and systems strengthening for child protection

General comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25

News articles

Daily Maverick, Bullied Limpopo schoolgirl's suicide raises disturbing questions about moral compass of our children, M le Cordeur, May 2021

Reports and General comments

International Telecommunication Union (2016), "Measuring the Information Society Report"

Internet Watch Foundation, Annual Report, 2022

F Gottschalk, 2019, Impacts of Technology Use on Children: Exploring Literature On The Brain, Cognition And Well-Being OECD Education Working Paper No. 195

Growing up in a connected world, UNICEF Office of Research – Innocenti, Florence, 2019

Websites

Human Rights watch, *Impact of Covid-19 on Children's Education in Africa* available at https://www.hrw.org/news/2020/08/26/impact-covid-19-childrens-education-africa
https://www.trustonic.com/opinion/what-are-the-barriers-to-smartphone-expansion-across-africa/#:~:text=In%20certain%20regions%20of%20Africa,all%20nations%20on%20the%20continent
'Racism for sale' BBC Africa Eye documentary, available at https://www.bbc.com/news/av/world-africa-61764466
National treasury, Budget 2023 Highlights. Available https://www.treasury.gov.za/documents/national%20budget/2023/sars/Budget%202023%20Highlights.pdf
Ten-year study shows South African school reading literacy is slow to improve, University of Pretoria, Available: https://www.up.ac.za/research-matters/article/2801832/ten-year-study-shows-south-african-school-reading-literacy-is-slow-to-improve
Draft policies information security policies available: https://www.gov.za/sites/default/files/gcis_document/201409/infosecure0.pdf

Ratification status of South Africa, available https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=162&Lang=EN

Ratification status to the ACRWC, available https://au.int/sites/default/files/treaties/36804-sl-AFRICAN_CHARTER_ON_THE_RIGHTS_AND_WELFARE_OF_THE_CHILD.pdf

S Miller 'Child protection in the digital world: Why is it needed?' 2023 https://www.savethechildren.net/blog/child-protection-digital-world-why-it-needed#:~:text=The%20fact%20is%20that%20the,relevant%20international%20laws%20%5B1%5D.

https://usa.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online