Global Campus Africa

Awarded Theses 2019/2020

Opal Masocha Sibanda

Protection of Children's Rights to Privacy and Freedom from Online Exploitation and Abuse in Southern Africa.

A Case Study of South Africa and Zimbabwe

HRDA, The Master's Programme in Human Rights and Democratisation in Africa

OPAL MASOCHA SIBANDA

PROTECTION OF CHILDREN'S RIGHTS TO PRIVACY AND FREEDOM FROM ONLINE EXPLOITATION AND ABUSE IN SOUTHERN AFRICA
A CASE STUDY OF SOUTH AFRICA AND ZIMBABWE

FOREWORD

The Global Campus of Human Rights is a unique network of more than one hundred participating universities around the world, seeking to advance human rights and democracy through regional and global cooperation for education and research. This global network is promoted through seven Regional Programmes which are based in Venice for Europe, in Sarajevo/Bologna for South East Europe, in Yerevan for the Caucasus, in Pretoria for Africa, in Bangkok for Asia-Pacific, in Buenos Aires for Latin America and the Caribbean, and in Beirut for the Arab World.

Every year each regional master's programmes select the best master thesis of the previous academic year that is published online as part of the GC publications. The selected seven GC master theses cover a range of different international human rights topics and challenges.

The Global Campus Awarded Theses of the academic year 2019/2020 are:

• Botazzi, María Florencia, *Mi derecho a tener derechos. Políticas públicas de autonomía progresiva y egreso dirigidas a adolescentes bajo cuidados alternativos en Santa Fe*, Supervisor: Javier Palummo, Universidad de la República, Uruguay. Master's Programme in Human Rights and Democratisation in Latin American and the Caribbean (LATMA), coordinated by National University of San Martin (Argentina).

• Hermus, Nina, *"Forgotten Victims of War". Invisible, though Stigmatised: the Case of Children Born of Wartime Rape and Conflict-Related Sexual Violence*, Supervisor: Kalliope Agapiou-Josephides, University of Cyprus. European Master's Programme in Human Rights and Democratisation (EMA), coordinated by Global Campus of Human Rights Headquarters.

• Kalem, Melina, *#Fridaysforfuture. Beyond the Hashtag on Youth Activism for Climate Justice: A Case Study of Slovenia's Youth for Climate Justice (Mladi Za Podnebno Pravičnost, MZZP)*, Supervisor: Mladen Domazet, Institute for Political Ecology (IPE, Croatia). European Regional Master's Programme in Democracy and Human Rights in South East Europe (ERMA), coordinated by University of Sarajevo and University of Bologna.

• Macharia, Wilson, *Access to Justice for Persons with Disabilities in Kenya: from Principles to Practice*, Supervisors: Benyam Dawit Mezmur, University of Western Cape and Susan Mutambasere, University of Pretoria. Master's Programme in Human Rights and Democratisation in Africa (HRDA), coordinated by Centre for Human Rights, University of Pretoria.

• Sibanda, Opal Masocha, *Protection of Children's Rights to Privacy and Freedom from Online Exploitation and Abuse in Southern Africa. A Case Study of South Africa and Zimbabwe,* Supervisors: Zahara Nampewo, Makerere University (Uganda) and Marystella Simiyu, University of Pretoria. Master's Programme in Human Rights and Democratisation in Africa (HRDA), coordinated by Centre for Human Rights, University of Pretoria.

• Van Der Werf, Charlotte Vera, *Lebanon's October Uprising: A Clean Slate for Syrian Refugees?* Supervisor: Zeina El-Hélou, Saint Joseph University (Lebanon). Arab Master's Programme in Democracy and Human Rights (ARMA), coordinated by Saint Joseph University (Lebanon).

• Yutthaworakool, Saittawut, *Understanding the Right to Change Legal Gender: A Case Study of Trans Women in Sri Lanka*, Supervisor: Kokila Lankathilake Konasinghe, University of Colombo (Sri Lanka) and Mike Hayes, Mahidol University. Master's Programme in Human Rights and Democratisation in Asia Pacific (APMA), coordinated by Mahidol University (Thailand).

This publication includes the thesis *Protection of Children's Rights to Privacy and Freedom from Online Exploitation and Abuse in Southern Africa. A Case Study of South Africa and Zimbabwe* written by Opal Masocha Sibanda and supervised by Zahara Nampewo, Makerere University (Uganda) and Marystella Simiyu, University of Pretoria.

BIOGRAPHY

Opal is a human rights lawyer from Zimbabwe with extensive experience in the child rights sector. She has interests in areas such as access to justice by children and children's rights in the digital age. She is currently a Legal Researcher at the Secretariat of the African Committee of Experts on the Rights and Welfare of the Child in Maseru, Lesotho.

ACKNOWLEDGEMENTS

I am forever thankful to God. Had it not been for his grace, I would not have made it. Ebenezer!

A big thank you to my family and friends for the support and encouragement. I have made it!

I wish to express my deepest gratitude to the Centre for Human Rights for giving me an opportunity to further my studies and advance my career.

I further extend my sincere gratitude to the European Union through the Global Campus of Human Rights, the Royal Norwegian Embassy in Pretoria, South Africa and the Right Livelihood Foundation for funding my studies.

A very special appreciation to my supervisors, Dr Zahara Nampewo and Marystella Simiyu for the guidance. I am indebted.

To my HRDA friends, thank you for making the year worthwhile. I wish you nothing but the best.

DEDICATION

Dedicated to my father. I know you are very proud of me.

ASTRACT

In the past few years there has been an increase in the number of children using the internet. The COVID-19 pandemic has further contributed to the increase in internet usage by children due to the measures taken by governments to contain and curb the virus, including the closure of schools. Families and children have resorted to digital solutions to support children's education, interaction and play. Although not universal, the internet presents various opportunities that enable children to enjoy their rights.

African countries including South Africa and Zimbabwe have embraced the use of internet based technologies which has created opportunities for cybercriminals to perpetuate violence against children. As such, whilst acknowledging the benefits of the internet, it should also be noted that the internet presents threats to children's rights, the most critical being threats to privacy and freedom from exploitation and abuse. Due to their age, children do not appreciate the threats presented by the internet and thus remain vulnerable internet users.

Various instruments exist at international and regional level on the protection of children's rights and these instruments also apply in the digital context. A number of laws have been enacted in South Africa and Zimbabwe on the protection of children's rights. It is however not doubted that the existing legislation and traditional governmental bodies set up to protect children from probable harm are challenged by technological advancements such as the internet.

This research establishes that the legal framework of South Africa and Zimbabwe does not adequately protect children's rights to privacy and freedom from online exploitation and abuse. Although South Africa has made notable progress in enacting laws on the protection of children's rights online, the laws are not comprehensive. Zimbabwe on the other hand is lagging behind in terms of amending its legislation to incorporate aspects of online violence. With weak legislation, protection of children's rights to privacy and freedom from online exploitation and abuse becomes problematic, hence the need for law reform. The research draws best practices from the legal regimes of the European Union and the United States of America to inform law reform. The research gives recommendations to the government of South Africa and Zimbabwe, businesses and internet service providers, as well as parents and guardians on the protection of children's rights online.

TABLE OF ABBREVIATIONS

ACRWC	African Charter on the Rights and Welfare of the Child
CIPA	Children's Internet Protection Act
CRC	Convention on the Rights of the Child
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and communications technology
ISPs	Internet service providers
ITU	International Telecommunications Unit
MISA	Media Institute of Southern Africa
OECD	Organisation for Economic Co-operation and Development
OPSC	Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography
POTRAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
SADC	Southern African Development Committee
UN	United Nations
UNCRC	United Nations Committee on the Rights of the Child
UNICEF	United Nations Children's Fund
USA	United States of America
USC	United States Code

TABLE OF CONTENTS

Foreword II
Biography IV
Astract VI
Table of abbreviations VII

1. INTRODUCTION 1
1.1 Background 1
1.2 Research problem 3
1.3 Research questions 4
1.4 Methodology 5
1.5 Limitations of the research 5
1.6 Literature review 5
1.6.1 Children and the internet 5
1.6.2 Legal frameworks in protecting the rights of children online 7
1.7 Definition of terms 9
1.8 Structure 10

2. CHILDREN AND THE INTERNET 11
2.1 Introduction 11
2.2 Snapshot on internet usage by children 12
2.3 Opportunities for children 15
2.3.1 Right to education 15
2.3.2 Participation and freedom of expression 16
2.3.3 Access to information 17
2.3.4 Leisure and recreation 17
2.4 Online risks, vulnerability and harm 17
2.4.1 Content risks 19
2.4.2 Contact risks 20
2.4.3 Conduct risks 21
2.4.4 Threats relating to privacy 23
2.5 Conclusion 24

3. USING THE LAW TO PROTECT CHILDREN'S RIGHTS TO PRIVACY AND FREEDOM FROM ONLINE EXPLOITATION AND ABUSE 25
3.1 Introduction 25
3.2 International legal framework 26
3.2.1 Convention on the Rights of the Child 27
3.2.2 Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography 30
3.2.3 Council of Europe's Convention on Cybercrime 31
3.2.4 Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse 31
3.2.5 International Telecommunications Unit Resolution 179 32
3.2.6 UN Guiding Principles on Business and Human Rights 32
3.3 Regional legal framework 33
3.3.1 African Charter on the Rights and Welfare of the Child 33
3.3.2 African Union Convention on Cyber Security and Personal Data Prevention 35
3.3.3 Southern African Development Committee model law on data protection and information and communications technology 35
3.4 National legal frameworks 36
3.4.1 Zimbabwe 36
3.4.2 South Africa 41
3.5 Conclusion 49

4. BEST PRACTICES FROM OTHER JURISDICTIONS 50
4.1 Introduction 50
4.2 Rationale for selected legal regimes 51
4.3 The European Union legal regime 52
4.3.1 General Data Protection Regulation 52
4.4 The United States of America legal regime 56
4.4.1 The United States Criminal Code 56
4.4.2 Children's Internet Protection Act 2000 59
4.5 Conclusion 60

5. CONCLUSION AND RECOMMENDATIONS 61
5.1 Conclusion 61
5.2 Recommendations 62
5.2.1 Recommendations to states 62
5.2.2 Recommendations to businesses and ISPs 64
5.2.3 Recommendations to parents and guardians 65

BIBLIOGRAPHY 66

#TOWARDSASAFERINTERNETFORCHILDREN

1.

INTRODUCTION

1.1 Background

Worldwide, an estimate of one in three internet users is below the age of 18 years.[1] Although there has been growth in internet usage by children in the past few years, the COVID-19 pandemic further contributed to the growth in the number of children accessing the internet. The pandemic pushed governments to pass measures that are meant to protect the public from contracting the virus. In Zimbabwe for example, section 4(1)(e) of the Public Health (COVID-19 Prevention, Containment & Treatment) (National Lockdown) Order SI 83 of 2020 provided that all schools were to remain closed with effect from 30 March 2020 to 19 April 2020. The period was extended due to the increase in COVID-19 cases. Schools, including those in South Africa and Zimbabwe, introduced technological solutions through online learning to ensure that children continue with their studies.[2] In this regard, it is acknowledged that the growth in access to technology has created various opportunities for children to enhance their rights such as the right to education among other rights.[3] Access to technology has

[1] S Livingstone, J Carr and J Byrne, 'One in Three: Internet Governance and Children's Rights' (Innocenti Discussion Paper 2016-01 UNICEF 2016) 7 <www.unicef-irc.org/publications/pdf/idp_2016_01.pdf> accessed 24 May 2020.

[2] United Nations Children's Fund (UNICEF) and others, 'Covid-19 and its implications for protecting children online' (UNICEF 2020) 1 <www.unicef.org/sites/default/files/2020-04/COVID-19-and-Its-Implications-for-Protecting-Children-Online.pdf> accessed 21 October 2020.

[3] S Livingstone and B O'Neill, 'Children's rights online: challenges, dilemmas and emerging directions' in S van der Hof, B van den Berg and B Schermer (eds), *Minding Minors Wandering the Web: Regulating Online Child Safety. Information technology and law series* (Springer Asser Press 2014) 19-38.

also ensured that children still have access to these rights in the event of emergencies, for example, the COVID-19 pandemic.

Whilst access to the internet has brought opportunities for children, the benefits present opportunities for children's rights violations online.[4] Among the threats to children online is the violation of children's rights to privacy and freedom from exploitation and abuse. Just like adults, being online can pose higher risk of interference with children's right to privacy. Most children upload general personal information and photos which will possibly be on the internet for long periods. Children's physical privacy is also affected by technologies through tracking, monitoring and broadcasting children's live images, behaviour or locations.[5] Children's digital footprints may also be manipulated by public authorities and companies may collect data relating to children. Governments on the other hand intercept children's communications for security reasons thereby infringing their right to privacy in the event that their personal data is collected, stored or processed.[6] Parents or other individuals may also share information concerning children thereby violating children's privacy.[7] This may include malicious sharing of children's images that may portray pornography and ridicule. Children are more susceptible to interferences into their privacy due to their inability to comprehend the long-term effects of sharing personal information online.[8] The mere fact that data on children can be collected from the time they are born, the large generation of digital information throughout the first 18 years of their life, and the numerous and evolving technological means for processing data relating to children all raise serious concerns on how best the right to privacy can be protected in the digital sphere.[9]

Regarding exploitation and abuse, children are in jeopardy of coming into contact with illicit content which is highly presented online. This includes child pornography, violent and racist material, and content

[4] Council of Europe Commissioner for Human Rights, 'Protecting children's rights in the digital age: An ever-growing challenge' (*Council of Europe*, 2014) <www.coe.int/en/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen-1> accessed 24 May 2020.

[5] UNICEF, 'Children's online privacy and freedom of expression' (Industry toolkit, UNICEF 2018) 8 <www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf> accessed 24 May 2020.

[6] ibid.

[7] ibid.

[8] ibid.

[9] ibid.

encouraging practices of self-harm. Children are also vulnerable to cyberbullying which has tragic repercussions on them. Online predators also contact children using false identities with the aim of abusing them including sexually, commonly known as grooming, and to recruit them for the purposes of child trafficking or production of child pornography. According to the 'South African Kids Online' report in 2016, 51.2% of the children interviewed reported that they had seen sexual images online and 30.5% had received a message of a sexual nature.[10] On the other hand, 20.5% of the children had received a message they did not want with advertisements for or links to x-rated websites, whilst 19.2% opened a message or link showing pictures of naked people or of people having sexual intercourse.[11] This is an example of the extent to which children's right to freedom from exploitation and abuse can be violated online hence the need to adopt effective measures to ensure the fulfilment of children's rights online.

1.2 Research problem

African countries including South Africa and Zimbabwe have fully embraced the use of internet based technologies which has created opportunities for cybercriminals to perpetuate violence against children.[12] Whilst a high number of attacks against internet users take place on a daily basis, only a small fraction of cybercrime is actually reported, prosecuted and adjudicated.[13] It is not doubted that the existing legislation and traditional governmental bodies set up to protect children from probable harm are challenged by technological advancements such as the internet hence the low numbers of prosecuted cases of online violence.[14] This is also a challenge in South Africa and

[10] P Burton, L Leoschut and J Phyfer, 'South African Kids Online: A glimpse into children's internet use and online activities' (The Centre for Justice and Crime Prevention 2016) 32-33. <www.cjcp.org.za/uploads/2/7/8/4/27845461/south_africa_kids_online_full_report.pdf> accessed 24 May 2020.

[11] ibid.

[12] N Kshreti, 'Cybercrime and Cyber Security in Africa' (2019) 22 Journal of Global Information Technology Management 78.

[13] J Kleijssen and P Perri, 'Cybercrime, Evidence and Territoriality: Issues and Options' in W Kuijer and W Werner (eds), *Netherlands Yearbook of International Law* (TMC Springer: Asser Press 2016) 47, 148.

[14] E Staksrud, *Children in Online World Risk, Regulation, Rights* (Ashgate 2013) 3.

Zimbabwe wherein the majority of online abuse cases are not reported and not known due to the lack of adequate legal frameworks to provide guidance and a standardised way of addressing violation of children's rights online. Although children's rights are provided for in the existing and pending legislation in South Africa and Zimbabwe, there are still gaps in the laws with regards to the protection of children's rights online hence posing challenges in the implementation of the law. Children on the other hand due to their inexperience and immaturity do not know how to identify online risks and protect themselves from online harm hence they remain at risk.[15] With weak legislation and enforcement, protection of the rights of children online becomes problematic as there is no guidance on how to prevent, respond to and reduce cybercrime.

1.3 Research questions

The research aims to answer the following main research question:

To what extent are children's rights to privacy and freedom from online exploitation and abuse protected in South Africa and Zimbabwe?

The following are sub-questions to the main research question:

1. What is the nature and scope of violation of children's rights to privacy and online abuse and the impacts thereof?
2. Do the legal frameworks of both countries adequately provide for the protection of children's rights to privacy and freedom from online exploitation and abuse?
3. What is the standard of best practice regarding the protection of children's rights to privacy and freedom from online exploitation and abuse?
4. What recommendations can be suggested to ensure the protection of children's rights online?

From the above, the researcher infers the main hypothesis that whilst children across the world inhabit the online environment in increasing numbers, the increase in access to the internet has resulted in increased risk to children's safety and security as they are exposed to many risks which might result in violation of their rights.

[15] Livingstone and O'Neill (n 3).

1.4 Methodology

The research is a qualitative research informed by desk review. Primary legal sources including treaties, conventions and legislation, as well as secondary legal sources like case law, journal articles, reports, papers and books were consulted. A systematic analysis to augment the findings was conducted on South Africa and Zimbabwe in order to guarantee a representative picture of the status of protection of children's rights to privacy and freedom from exploitation and abuse in the digital sphere in the two countries. Best practices were drawn from other jurisdictions to inform law reform.

1.5 Limitations of the research

The research only focuses on two countries in Southern Africa – South Africa and Zimbabwe. The rationale is that South Africa has legislation that protects children's rights online including the Cybercrime Bill that was recently passed whilst Zimbabwe has a pending Cybercrime Bill. The two legal systems are comparable and best practices can be drawn from South Africa. The research is based on desktop research and revision of existing literature. The COVID-19 pandemic has impacted on the methodology as physical interviews could not be conducted with key respondents of the research. Further, there is no information on children's internet usage in Zimbabwe unlike in South Africa. As such, much reference is made to South Africa when discussing children's online practises.

1.6 Literature review

1.6.1 Children and the internet

The 'South African Kids Online' report gives an insight about children's online practises, online opportunities and risks for children. Access to the internet creates opportunities which includes various domains, including education, communication, creativeness and

entertainment.[16] These opportunities enable children to advance their abilities and learn on their own terms through means whereby they can possibly avoid the limitations and demands of their life offline, thereby building their independence.[17]

The Organisation for Economic Co-operation and Development (OECD) report on the protection of children's rights online categorises online risks for children. Firstly, the report refers to internet technology risks wherein a child is exposed to content or where there is communication on the internet. The second category is consumer-related risks wherein the child becomes a targeted consumer online. The third category is information privacy and security risks. These risks are faced by most internet users but children are the most vulnerable group.[18] According to the report, online risks have different consequences on children, the most severe being physical and psychological harm.[19] Economic effects and long-term risks such as enduring disadvantageous personal information online must also not be underestimated.[20]

Whilst the two reports are comprehensive in respect to online opportunities and risks, the challenge is that the opportunities and risks are not explicitly linked to children's rights. The reports only mention that children enjoy their right to freedom of expression and right to receive information. There are however some rights enjoyed by children online such as the rights to education, leisure and recreation, freedom of speech and freedom of association. It is therefore the objective of this research to clearly link the specific children's rights with the opportunities and risks created by the internet. The research will clearly show which rights are enjoyed by children through the opportunities they have online and the rights that are violated by online harms.

[16] Burton, Leoschut and Phyfer (n 10).
[17] ibid.
[18] OECD, 'The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them' (OECD 2011) 24 <www.oecd-ilibrary.org/science-and-technology/the-protection-of-children-online_5kgcjf71pl28-en> accessed 24 May 2020.
[19] ibid 39.
[20] ibid.

1.6.2 Legal frameworks in protecting the rights of children online

Bryne and Burton state that the United Nations Convention on the Rights of the Child (CRC),[21] is the most comprehensive human rights framework for advancing the rights of children as it makes provision for the protection, provision and participation rights of children in relation to technologies.[22] They recognise that access to the internet promotes the right to access information and freedom of speech and can be considered as a principal prerequisite for facilitating the fulfilment of other digital rights.[23] They however argue that there have been growing concerns among scholars and professionals that the available international and domestic online related policies do not sufficiently address children's issues online.[24] They also argue that the available policies on children's rights and welfare do not take into consideration the emerging evidence regarding the opportunities associated with internet usage by children such as education, freedom of expression, access to information and civic engagement.[25]

In the Children's Commissioner for England report, it is argued that although the CRC provides comprehensive protection of children's rights, it was adopted in 1989 when there was not much internet access by children.[26] The rights stated in the CRC thus do not make reference to digital engagement despite the fact that nowadays children spend most of their time online.[27] It is suggested that the CRC should be updated so it can fit within the digital context.

Kshreti highlights that there is weak legislation and enforcement of the law on cybercrime in Africa hence the low figures of reported, prosecuted and adjudicated cases on cybercrime.[28] He makes reference to a report of the African Union Commission and Symantec which indicated that in 2016, 30 African countries lacked explicit legal provisions to fight

[21] Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC).

[22] J Byrne and P Burton, 'Children as Internet users: how can evidence better inform policy debate?' (2017) 2 Journal of Cyber Policy 40.

[23] ibid.

[24] ibid.

[25] ibid.

[26] Children's Commissioner of England, 'Growing Up Digital: A report of the Growing Up Digital Taskforce' (Children's Commissioner of England 2017) 16 <www.childrenscommissioner.gov.uk/report/growing-up-digital/> accessed 24 May 2020.

[27] ibid.

[28] Kshreti (n 12).

cybercrime.[29] The challenge with Kshreti's article is that it is broad and covers general aspects of cybercrime in Africa thereby failing to shed more light on the manner in which children's rights are affected and how the existing legislation protects children from online abuse.

The 'South African Kids Online' report briefly discusses the existing legal frameworks on protecting the rights of children online. According to the report, a few laws and policies in South Africa directly address children's rights online.[30] The report concludes that although there are some laws addressing children's rights online and protection of children, the existing laws are far from comprehensive.[31] The challenge in the legislation is the inability to differentiate between the production of child sexual abuse materials and consensual sexting amongst children. This is unreasonably retributive of normal sexual development and can be regarded as infringing on children's rights online.[32] The report calls for law reform to better handle the intricacy of online victimisation and ensure that children enjoy their rights offered by the internet. It is essential to note that whilst the report discusses the existing laws on protection of children, it does not offer a broad discussion of the strengths and gaps in the existing legal frameworks in protecting children's rights to privacy and freedom from exploitation and abuse online.

It is also important to note that there is scant literature on the protection of children's rights online by the current legislation in Zimbabwe. Furthermore, there have been recent developments in law reform as South Africa and Zimbabwe both have Cybercrime Bills. There is not much information on the analysis of both bills. Also looking at the regional level, there has been not much literature on the extent to which the available legal instruments protect children's rights in the digital context.

It is the purpose of this research to give an overview of children's online practises, opportunities and risks as well as to comprehensively analyse the legal frameworks on the protection of children's rights on the internet with focus on privacy, exploitation and abuse. It is intended that the research will contribute to existing literature and will be utilised in lobbying and advocating for the promotion and protection of children's rights in the digital age in South Africa and Zimbabwe.

[29] African Union Commission (AUC) and Symantec 'Cyber Crime and Cybersecurity Trends in Africa' (AUC and Symantec 2016) 53.
[30] Burton, Leoschut and Phyfer (n 10) 4-6.
[31] ibid.
[32] ibid.

1.7 Definition of terms

Access to the internet – this refers to children who have used the internet or have been online.[33]

Digital or online rights – this refers to human rights that enable individuals to access and use computers or other electronic devices and the internet.[34]

Internet or online – this refers to a global computer network providing various information and communication facilities, comprising of interconnected networks using standardised communication protocols.[35]

Online exploitation and abuse – online exploitation can be used to capture all types of offences that take place in the online environment. This includes online grooming, live streaming,online coercion and child pornography.[36] Online abuse refers to any type of abuse that can happen on the internet for example cyberbullying.[37]

Online harm – this refers to online behaviour that may hurt a child physically or emotionally. This can be harmful information posted online or sent directly to a child.[38]

Opportunities – this refers to the positive experiences that children find online.[39]

Risks – this refers to negative experiences found by children online.[40]

[33] Ghana Country Report, 'Risks and opportunities related to child online practices' (2017) 17 <www.unicef.org/ghana/media/1791/file/Risks%20and%20Opportunities%20-%20Child%20Online%20Protection.pdf> accessed 16 August 2020.

[34] Lexico Oxford English and Spanish Dictionary, 'Internet' (*Lexico*) <www.lexico.com/definition/internet> accessed 12 August 2020.

[35] Ghana Country Report (n 33).

[36] Child exploitation and Online Protection command, 'What is Online Child Sexual Abuse and Exploitation?' <www.ceop.police.uk/Safety-Centre/what-is-online-child-sexual-abuse/> accessed 16 August 2020.

[37] NSPCC, 'Online abuse' (*NSPCC*) <www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/online-abuse/> accessed 16 August 2020.

[38] Ghana Country Report (n 33).

[39] ibid.

[40] ibid.

1.8 Structure

The research is made up of five chapters. The first chapter gives a background and introduction of the topic, research problem, research questions, methodology and limitations of the study, literature review and definition of terms. The second chapter gives an overview of children's online practises, opportunities, risks and harms, and potential impact of the risks. The third chapter analyses the extent to which children's rights to privacy and freedom from online exploitation and abuse are protected in the international, regional and national legal frameworks. The fourth chapter provides best practices to inform law reform whilst the fifth chapter provides a conclusion and recommendations.

2.

CHILDREN AND THE INTERNET

2.1 Introduction

As established in the previous chapter, there has been growth in internet access by children over the past few years. Recently, the COVID-19 pandemic briskly pushed children's daily lives online due to the extensive physical and social distancing measures introduced by governments to contain and curb the virus, including widespread closure of schools.[41] Online platforms became the new normal as families, schools and children resorted to digital solutions to support children's education, interactions and play.[42] Whilst digital solutions create opportunities ensuring the continued enjoyment of children's rights, they also increase children's exposure to online risks and harms which have negative impacts on children.[43]

This chapter discusses children's online practices, risks, harms and impact. The chapter begins with an overview of the degree of internet usage by children. This is followed by a discussion of the opportunities available online for children, the potential risks and harms and their impact on children.

[41] UNICEF and others, 'Covid-19 and its implications for protecting children online' (UNICEF 2020) 1 <www.unicef.org/sites/default/files/2020-04/COVID-19-and-Its-Implications-for-Protecting-Children-Online.pdf> accessed 21 October 2020.
[42] ibid.
[43] ibid.

2.2 Snapshot on internet usage by children

For one to understand online opportunities, risks, harms and impacts, it is important to have a clear picture of the degree of internet access and usage by children.

According to a study conducted by the United Nations Children's Fund (UNICEF) in 2017, globally, youth aged between 15 and 24 are the most connected age group.[44] As at March 2020, internet penetration in Africa was at 39.3 % of the entire populace compared to the rest of the world at 62.9%.[45] During the first quarter of 2020, Zimbabwe had a mobile penetration rate of 94.2% and active internet penetration rate of 59.1%.[46] In South Africa, the Independent Communications Authority revealed that mobile penetration reached 91.2% in 2019 and the internet penetration rate was 62% in January 2020. According to the UNICEF 2017 study, 60% of the youth in Africa are not connected to the internet as compared to Europe which only has 4% of youths not connected.[47] The available information on the degree of internet and mobile phone usage is however likely to be quickly outdated given the emergence of smartphones and the increase in the number of children using the internet.[48]

There is currently no available data on internet usage by children in Zimbabwe although the Postal and Telecommunications Regulatory Authority of Zimbabwe report highlighted that 40.5% of the population used the internet to access WhatsApp in the beginning of 2020.[49] In South Africa, the following information was noted from a study conducted around 2016 in Gauteng, Eastern Cape and Western

[44] UNICEF, *The State of the World's Children* (UNICEF 2017) <www.unicef.org/reports/state-worlds-children-2017> accessed 8 September 2020.

[45] Polity, 'Delivering education online: coronavirus underscores what's missing in Africa' (*Polity*, 20 April 2020) <www.polity.org.za/article/delivering-education-online-coronavirus-underscores-whats-missing-in-africa-2020-04-20> accessed 8 September 2020.

[46] Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), 'Abridged Postal & Telecommunications Sector Performance Report First Quarter' (POTRAZ 2020) <www.potraz.gov.zw/wp-content/uploads/2020/06/Sector_Performance_1stQ2020.pdf> accessed 8 September 2020.

[47] UNICEF, *The State of the World's Children* (n 44).

[48] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (UNICEF 2012) 19 <www.unicef-irc.org/publications/652-child-safety-online-global-challenges-and-strategies-technical-report.html> accessed 13 September 2020.

[49] POTRAZ (n 46).

Cape, both in urban and rural settings.[50] The children interviewed were aged between nine and seventeen years. The study is however not representative of South Africa wholly.

- 70.4% used the internet whilst 29.6% did not;
- 51.2% who could not access the internet indicated that their parents or guardians would not allow them whilst 37.1% indicated that the cost of devices and data was high;
- 80.2% accessed the internet using smartphones. Desktops, laptops and tablets were not used frequently;
- 49.9% played online games, 51.8% watched video clips and 64.2% visited social networking sites;
- 70% used the internet for school work whilst 45% looked for information on study and work opportunities;
- 64% used the internet for communication;
- 86.3% had accounts on social networking sites; WhatsApp 94.2%, Facebook 68.5% and Instagram 18.0%;
- 40.1% had their profiles set to private on social media platforms, with only friends seeing information they shared;
- 46.0% had used privacy settings, with 49.4% having had an intention to block someone;
- 51.2% of nine to eleven year olds knew the type of information they should share or not share online, 56.9% knew how to remove a person from their contact list and 41.0% knew how to change sharing settings on social media. Almost all 15-17 year olds knew how to perform these tasks;
- 33.6% would accept a contact only if they knew the person concerned and 25.4% would accept a contact only if the person was well known to them;
- 83.8% owned devices, with a large number of older children (92.5%) having their own devices as opposed to younger children; and
- 48.1% of the children never engaged with their parents about their internet usage whilst 57.0% of the parents indicated that they never communicated with their children about safe use of the internet.

[50] J Phyfer, P Burton and L Leoschut, 'South African Kids Online: Barriers, opportunities and risks. A glimpse into South African children's internet use and online activities' (Technical report, Centre for Justice and Crime Prevention 2016) 12 <http://eprints.lse.ac.uk/71267/2/GKO_Country-Report_South-Africa_CJCP_upload.pdf> accessed 13 September 2020.

An analysis of the data above shows that a high number of children have access to the internet and for those who cannot, the barriers range from parental controls and lack of funds to purchase devices or data. It can also be noted that most children access the internet through smartphones as opposed to computers. Whilst it is appreciated that smartphones are convenient, it has been argued that a bedroom culture has been fuelled by the use of smartphones hence making access to the internet by children more private, personal and with minimal supervision hence exposing children to online risks.[51] This assertion is strengthened by the study which revealed that most parents expressed being helpless around supervising their children online especially where the child concerned had a personal device.[52]

A further analysis indicates that children explore the internet for entertainment, learning and for social purposes. WhatsApp and Facebook are the most popular social networking sites amongst children. Social media usage however varies with age as it was reported that only 31.5% of the children aged between nine and eleven used Facebook as compared to 83.5% of the children aged between 15 and 17.

Regarding skills, whilst some children, especially older ones display digital skills and knowledge on keeping safe online, other children, mostly young ones lack those skills hence making themselves susceptible to online risks. For instance, the study revealed that when social networking and using online gaming sites, 13.3% of the children had used the report button whilst 49.4% had used the blocking button.

According to the study, young children used the internet to a lesser extent than older children; 115 children aged between nine to eleven years compared to 232 children aged 12-14 years and 293 children aged 15-17 years.[53] It can therefore be noted that internet usage by children, online behavioural traits and vulnerabilities differ according to their ages.

The data also indicates that there is less parental involvement in internet usage by children. This can be a factor that contributes to children's vulnerability online as they are not supervised or educated about the dangers available on the internet.[54]

[51] UNICEF, *The State of the World's Children* (n 44) 64.
[52] Phyfer, Burton and Leoschut (n 50) 70.
[53] ibid 14.
[54] ibid.

2.3 Opportunities for children

Access to the internet presents opportunities for the fulfilment of children's rights through. It is however imperative to highlight that there is a digital divide which has resulted in some children not benefitting from the opportunities created by the internet due to various reasons that limit their access to the internet. Reasons for the digital divide can be geographical, financial, digital literacy and gender related.[55] In Zimbabwe for example, less than 5% of children below 15 years use the internet.[56] The UNICEF study also revealed that rural children do not have access to the internet unlike those living in the urban areas,[57] whilst the existence of financial gaps also pose challenges as children from wealthy families have more access to the internet than those from poor backgrounds.[58] Further, with the emergence of smartphones and many children using them, it has been argued that smartphones offer a 'second best' online experience and are not 'functionally equivalent substitutes' for personal computers. There are constraints associated with the use of smart phones to access the internet mostly for tasks related to creating content such as long-form writing, video design and editing.[59] On the other hand, children who are not digitally literate or speak minority languages might not be able to access relevant information online.[60] Lastly, gender gaps in some countries have resulted in females having less access to the internet than males.[61] It should therefore be borne in mind that the opportunities created by the internet are not enjoyed by all children.

Below, although not universal, are the rights enjoyed by children as they navigate the internet.

2.3.1 Right to education

Access to the internet can change children's learning opportunities, skills and access to information thereby promoting their right to education. The fact that children can have access to significant

[55] UNICEF, *The State of the World's Children* (n 44).
[56] ibid.
[57] ibid.
[58] ibid.
[59] ibid 55.
[60] ibid.
[61] ibid.

information in the internet has a progressive bearing on the promotion of their right to education.[62] According to the 'South African Kids Online' report, 49.9% of the children revealed that they enjoyed using the internet due to the learning opportunities it presented.[63] Further, 58.4% of the children used the internet at least on a weekly basis for school work.[64] Other children highlighted that they were able to have group work and conduct discussions online.[65] With the closure of schools during the COVID-19 pandemic, some schools in South Africa and Zimbabwe resorted to online learning, enabling children to enjoy their right to education amid the pandemic. Children can access books in online libraries such as Amazon and learn on online platforms such as Zoom and Google Meets.[66] The internet has thus ensured the continued enjoyment of the right to education even in times of emergencies.

2.3.2 Participation and freedom of expression

Online platforms create prospects for civic engagement and freedom of expression among children.[67] There have been traditional barriers in participation linked to gender, disability and age but, however, online platforms can overcome these barriers in societies where there is exclusion of particular groups from being involved in decision making on issues affecting them.[68] The internet presents changes to children with disabilities and children who are excluded and marginalised due to age, ethnicity or gender identities.[69] Children with disabilities who are usually secluded and face stigma, discrimination and a social setting that does not accommodate their needs can share their views and take part in matters affecting them online. The internet can create an opportunity for connection with peers, political engagement and partaking in

[62] S Livingstone, J Carr and J Byrne, 'One in Three: Internet Governance and Children's Rights' (Innocenti Discussion Paper 2016-01 UNICEF 2016) 7 <www.unicef-irc.org/publications/pdf/idp_2016_01.pdf> accessed 24 May 2020.
[63] Phyfer, Burton and Leoschut (n 50) 22.
[64] ibid 28.
[65] ibid.
[66] M Jantjies, 'Kids can keep learning even during a lockdown. Here is how' (*The Conversation*, 26 March 2020) <https://theconversation.com/kids-can-keep-learning-even-during-a-lockdown-heres-how-134434> accessed 24 May 2020.
[67] Livingstone, Carr and Byrne (n 62) 23.
[68] ibid.
[69] UNICEF, *The State of the World's Children* (n 44) 30.

decision making for excluded groups of children in physical settings.[70] Children are able to participate in matters affecting them in various ways such as social networking, storytelling and blogging among other things, thereby enjoying their right to participation and freedom of expression.[71]

2.3.3 Access to information

Children have access to diverse knowledge and information on the internet. Some of the available information online is important for children's education or for their wellbeing for example sexual reproductive health.[72] Children can have access to information on sites such as Google and YouTube.

2.3.4 Leisure and recreation

The internet can also provide a huge opportunity for children to enjoy their right to leisure and recreation. Furthermore, children are gradually designers of online material which includes texts, animations, images, videos, blogs and applications.[73] To achieve this, children require opportunities to learn to create, code and share information and such opportunities are available in the internet.[74] Children can also play games, listen to music and watch movies online thereby enjoying their right to leisure and recreation.

2.4 Online risks, vulnerability and harm

Whilst the internet presents opportunities for children, it also presents numerous threats, the most critical being threats to their privacy and freedom from exploitation and abuse. According to the Microsoft 2019 Digital Civility Index, teenagers, especially girls, are affected by online risks.[75] Online harm takes a new dimension, partially as a result

[70] Livingstone, Carr and Byrne (n 62) 23.
[71] ibid.
[72] ibid.
[73] ibid.
[74] ibid.
[75] Microsoft, 'Digital Civility Index' (*Microsoft*, 2019) <www.microsoft.com/en-us/digital-skills/digital-civility?activetab=dci_reports%3aprimaryr5> accessed 8 September 2020.

of the nature of the internet for instance, the fact that information may stay online for long periods – and partially for the reason that children become far less self-conscious of their behaviour online than they are offline and may blame themselves for being exposed to harm.[76] Further, the protection of reputation online is a gradually contentious legal and political question and the internet has changed the concept of managing repute by intensely increasing the scale, scope and reach of information.[77]

Platforms that pose risks to children are texting apps such as WhatsApp; photo and video sharing apps such as Tik Tok, Instagram and Facebook; microblogging apps and sites such as Tumblr and Twitter; chatting, meeting and dating apps and sites such as Tinder; livestreaming video apps such as house party-group video chat and self-destructing apps such as SnapChat.[78] New technologies such as cryptocurrencies and the dark web are also increasing live streaming of child sexual abuse and other harmful content, posing challenges on law enforcement.[79] Online gaming sites also pose risks to children as some games are meant for adults and may contain inappropriate themes, images and language.[80]

Although there is growing evidence on the nature of online risks and harms, there is a need to distinguish between conduct portrayed as being risky and the likely harm related to the risks. Children may encounter or take risks but not suffer harm. Children may share personal information online which may be considered as risky behaviour but only a few children are likely to suffer any substantial harm.[81] Online risks on children can be classified as follows:

[76] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (n 48) 42.

[77] UNICEF, 'Children's Rights and Business in a Digital World: Privacy, protection of personal information and reputation' (Discussion Paper Series, UNICEF 2017) 17 <www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf> accessed 12 September 2020.

[78] C Elgersma, 'Parenting, Media, and Everything in Between: 18 Social Media Apps and Sites Kids Are Using Right Now' (*Common Sense Media*, 6 June 2019) <www.commonsensemedia.org/blog/16-apps-and-websites-kids-are-heading-to-after-facebook> accessed 14 September 2020.

[79] UNICEF, 'Children's Rights and Business in a Digital World: Privacy, protection of personal information and reputation' (n 77).

[80] NI Direct, 'Social media, online gaming and keeping children safe online' (*NI Direct*) <www.nidirect.gov.uk/articles/social-media-online-gaming-and-keeping-children-safe-online> accessed 14 September 2020.

[81] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (n 48) 26.

- Content – children have no active role in the process but merely receive general information such as advertising or spam; ferocious, horrific or hateful content; pornographic or harmful sexual content;[82]
- Contact – children are targeted as participants in individualised activity either by other children or adults; and
- Conduct – children are the initiators of risk-taking behaviour such as sharing pornographic material, sharing personal information and sexting.[83]

2.4.1 Content risks

Illegal content

Children can be exposed to illegal content on the internet. Examples can be promotion of racism, hate speech and other forms of discrimination. Content related to child pornography is also illegal content which children may come across online. It is however important to note that content that is illegal to publish or share varies across jurisdictions.[84]

Age-inappropriate content

Children can also be exposed to age-inappropriate content such as hate, violence or adult pornography. Children can inadvertently come across such content or purposely search for it as they take part in interactive media, such as online video games. Although not illegal, such content has effects on children's development.[85] Sometimes content which is harmful to children targets them, for instance through the use of misleading domain names. In some instances, it has been discovered that some websites encouraging hatred feature sections for children, with games and misinformation targeted at them.[86]

[82] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (n 48) 26..

[83] ibid.

[84] OECD, 'The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them' (OECD 2011) 17, 24 <www.oecd-ilibrary.org/science-and-technology/the-protection-of-children-online_5kgcjf71pl28-en> accessed 24 May 2020.

[85] ibid.

[86] J Dooley, J Pyzalski J and D Cross, 'Cyberbullying versus face-to-face bullying: A theoretical and conceptual review' (2009) 4 Journal of Psychology 106.

Harmful advice

Children can also receive harmful advice on the internet such as commission of suicide, drug and alcohol abuse, eating disorders and inflicting harm upon themselves which may harm them physically or emotionally.

2.4.2 Contact risks

Online grooming

A child can be befriended by an adult who builds an emotional connection with the child with future intentions of sexual exploitation and abuse or trafficking.[87] Usually, groomers use fake identities and victims are approached in child-friendly websites or social platforms, leaving children vulnerable and unaware of the fact that they have been approached for purposes of grooming.[88] Cases of grooming are increasing due to the anonymity and accessibility of digital technology which allows groomers to approach many children at once.[89] Grooming has negative impacts on children which may include anxiety and depression, suicidal thoughts and post-traumatic stress among other things.[90]

Child pornography

Children can be subject to child pornography, also referred to as child sexual abuse material, whereby material portraying acts of sexual abuse or children's genitalia is shared online. Such material can be in the form of images or videos.[91] Whilst such material has been sold for financial gain, other abusers have been sharing the material for free.[92] Exposure to pornography may result in negative consequences such as undermining recognised societal standards and perceptions about sexual conduct, earlier sexual activity, promiscuous behaviour, sexual deviancy, sexual offending and sexually compulsive behaviour.[93]

[87] ChildSafeNet, 'Cyber Grooming' (*ChildSafeNet*) <www.childsafenet.org/new-page-15> accessed 22 August 2020.

[88] ibid.

[89] ibid.

[90] NSPCC, 'Grooming' (*NSPCC*) <www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/> accessed 21 August 2020.

[91] ECPAT International and Religions for Peace, 'Protecting Children from Online Sexual Exploitation' (ECPAT International and Religions for Peace 2016) 7 <www.unicef.org/media/66776/file/Guide-for-Religious-Leaders-and-Communities-ENG.pdf> accessed 21 August 2020.

[92] ibid.

[93] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (n 48) 42.

Cyberbullying

Cyberbullying is another rampant risk faced by children online. Unlike physical bullying which takes place in public spaces where the child is among other children, the existence of the internet and the fact that most children always have their phones switched on denotes that public space is redefined to invade the child's home and creates avenues for the perpetrator to have possible unrestricted contact with the child involved.[94] Children who are victims of cyberbullying usually experience psychological distress and poor psychosocial adjustment misery, worry, confusion, anger, insecurity and, lowered self-esteem.[95] Cyberbullying has also contributed to poor performance at school and dropping out and in some rare instances led to suicide.[96] Additionally, cyberbullying may be more detrimental to the emotional development and wellbeing of children than offline bullying due to the likelihood of the abusive information being distributed through various internet platforms, causing extensive humiliation and exposure of the target.[97] There is an existence of a greater power inequality, with victims sometimes not aware of the identity of the bully, and with the bully having all-pervasive access in terms of space and time.[98]

2.4.3 Conduct risks

Sharing personal information

Children share and disclose personal information to the whole internet or with peers especially on social media platforms.[99] They are usually not aware of the range and breadth of the audience online and the potential danger that may result from such actions.[100] They assume that the information will always be within the boundaries of their close contacts, failing to anticipate the possibility of such information being shared. In some places, a significant number of teenagers upload personal images that have a sexual tone without awareness of the nature

[94] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (n 48) 44.
[95] ibid.
[96] J Raskauskas and AD Stoltz, 'Involvement in Traditional and Electronic Bullying among Adolescents Developmental Psychology' (2007) 43 American Psychological Association 564, 564–75.
[97] ibid.
[98] ibid.
[99] OECD (n 84) 27-28.
[100] ibid.

of the images and how they can be accessed and misused for sexual gratification purposes.[101] In worst cases, photos of children have been captured and shared within social networking sites for child sexual abuse material.[102] Even in scenarios where pictures have been voluntarily posted by children, they may not be aware of the possibility of their photographs later resurfacing should their lives or personal situations become of public interest.[103]

Sharing of problematic content

Children create, post and share problematic content online. Problematic content can be in the form of images or videos portraying group or self-inflicted violence.[104] Further, concerns have been raised about the extent to which most adolescents are using their smartphones for sexual communication and exploration. Precisely, concern has focused on 'sexting', that is whereby teenagers create and share sexually suggestive nude or semi-nude photos amongst themselves.[105] Sharing of such images may create threats to children's privacy and may lead to sexual exploitation and harassment. There have also been circumstances where children have committed suicide due to the unauthorised sharing of their pictures online resulting from sexting. A 14 year old girl from Zimbabwe committed suicide after her nude pictures were leaked on social media.[106]

Chatting with strangers

The study in South Africa revealed that young girls have resorted to chat rooms as opposed to face-to-face communication which is usually condemned by parents and guardians as a measure of preventing violence and risk in offline environments. Girls are spending time in their rooms interacting with unknown people in chat rooms. Additional risks are created by online gaming sites where children interact with strangers. Unlike in other platforms where children interact with people they know, children interact with total strangers in chat rooms and

[101] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (n 48) 28.
[102] UNICEF, *The State of the World's Children* (n 44).
[103] ibid.
[104] OECD (n 84) 24.
[105] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (n 48) 30.
[106] Save the Children, 'Children's online safety a priority in Zimbabwe' (*Save the Children Zimbabwe*, 1 November 2018) <https://zimbabwe.savethechildren.net/news/childrens-online-safety-priority-zimbabwe> accessed 21 August 2020.

gaming communities.[107] Children can end up being sexually exploited or bullied as a result of communicating with strangers online.

2.4.4 Threats relating to privacy

Information privacy risks exist for all internet users, with children being the most vulnerable due to lack of capacity and awareness on the implications attached to sharing their personal information online.[108]

Online surveillance

The internet creates new opportunities for companies and governments to collect, store and process children's data online.[109] Of particular concern with regards to children's privacy is the increasing use of mass surveillance strategies by companies and governments which collect the personal data and information of internet users including children. Online surveillance can be more dangerous to children as through bulk data collection, authorities are allowed to build and store records of children's digital footprints if linked to individual profiles.[110]

Biometrics, internet of things-enabled devices and blockchain

Children's privacy can also be affected by the use of biometrics. Biometrics are mostly used for identification purposes for example in migration or birth registration in states that do not have proficient birth registration systems.[111] There is now a combination of biometrics with online technologies such as social networks, internet of things, enabled devices and blockchain. Examples can be the integration of facial and voice recognition technologies that enable the identification of children's images and their voices.[112] A number of concerns have been raised over biometrics in addition to pre-existing risks relating to identity theft as well as ill-usage of personal data. The risks increase as a result of the permanent nature of biometric data.[113]

[107] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (n 48) 28.
[108] OECD (n 84) 26.
[109] MV Cunha, 'Child Privacy in the Age of the Web 2.0 and 3.0: Challenges and opportunities for policy' (Innocenti Discussion Paper 2017-03 UNICEF 2017) 8 <www.unicef-irc.org/publications/926-child-privacy-in-the-age-of-web-20-and-30-challenges-and-opportunities-for-policy.html> accessed 21 August 2020.
[110] ibid.
[111] ibid.
[112] ibid.
[113] ibid.

Sharenting

Threats to the privacy of children do not arise from companies and governments only. There are cases whereby parents' conduct online poses a threat to children's privacy. Cases of 'sharenting' whereby parents share their children's personal information or images have become very common. This form of parental breach of children's privacy can have another dimension in the digital era.[114] Sharenting has a bearing on a child's reputation or privacy either immediately or in the future, for instance, by enabling the abuse of such information.[115] On the other hand, children can be harassed as a result of their parents' information online or violation of their parents' rights online.

2.5 Conclusion

Access to the internet, although not universal, has contributed towards the enjoyment of children's rights online even in times of emergencies. However, the opportunities have made children vulnerable to various online risks and harms that have negative impacts on children's emotional, physical and psychological wellbeing. There is a need for legislative frameworks that ensure that children's rights to privacy and freedom from exploitation and abuse are protected online in as much as they are protected offline. The next chapter therefore discusses the various laws that have been enacted at international and domestic level and their effectiveness thereof.

[114] Cunha (n 109) 10.
[115] ibid.

3.

USING THE LAW TO PROTECT CHILDREN'S RIGHTS TO PRIVACY AND FREEDOM FROM ONLINE EXPLOITATION AND ABUSE

3.1 Introduction

The increase in internet usage by children and the threats posed discussed in the preceding chapters show how technological advancements such as the internet can have potential negative implications on the protection of children's rights. There is no doubt that the existing legal frameworks that seek to protect children's rights cannot adequately protect children's rights in the digital context due to the forms of abuse facilitated by the development of information technologies.[116] This calls for amendments to the existing laws to ensure that the threats to children's privacy and forms of exploitation of children caused by the digital technologies are appropriately addressed.[117]

This chapter seeks to analyse the legal frameworks on the protection of children's rights online and, in particular, which instruments have been implemented to protect children's rights to privacy and freedom from online exploitation and abuse. The chapter begins by discussing the international and regional instruments. This is followed by a discussion of Zimbabwe and South Africa's legal frameworks. Focus will be on laws and provisions relating to internet usage, privacy and protection from exploitation. Gaps and challenges in the laws will be identified.

[116] K Jaishankar, *Cyber criminology: Exploring Internet Crimes and Criminal Behaviour* (CRC Press 2011) 393.
[117] ibid.

3.2 International legal framework

The main instruments that are relevant to children's rights to privacy and freedom from exploitation and abuse are the CRC and the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OPSC).[118] Other relevant instruments are the Council of Europe Convention on Cybercrime[119]and Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Child Protection Convention)[120](both open for ratification by non-member states), International Telecommunications Unit (ITU) Resolution 179[121], and the UN Guiding Principles for Businesses and Human Rights (Guiding Principles).[122]

The United Nations Committee on the Rights of the Child (UNCRC) is also in the process of drafting General Comment 25,[123] to articulate ways in which children's rights provided for in the CRC are impacted both positively and negatively in and by the digital sphere and the subsequent state obligations and roles of non-state actors, mainly businesses, in this regard.[124]

[118] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (adopted 25 May 2000, entered into force 18 January 2002) A/RES/54/263) (OPSC).

[119] Council of Europe Convention on Cybercrime 2001 (Budapest Convention) (ECHR).

[120] Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Child Protection Convention) (ECHR).

[121] International Telecommunication Union Resolution 179 (REV.BUSAN, 2014) (ITU).

[122] UN Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework as annexed to the Report of the Special Representative of the United Nations Secretary-General on the issue of human rights and transnational corporations and other business enterprises (21 March 2011) A/HRC/17/31, United Nations, endorsed by the United Nations Human Rights Council in A/HRC/RES/17/4.

[123] UNCRC Draft General Comment 25 on children's rights in relation to the digital environment (2020).

[124] Global Partners Digital, 'UN Committee on the Rights of the Child: Concept note for a General Comment on children's rights in relation to the digital environment' (Global Partners Digital Submission 2019) <www.gp-digital.org/wp-content/uploads/2019/05/CRC-Children%E2%80%99s-Rights-in-Relation-to-the-Digital-Environment-GPD-Submission-GPD-Template-1.pdf> accessed 13 September 2020.

3.2.1 Convention on the Rights of the Child

The CRC, which is nearly universally ratified,[125] provides a framework on the protection of children's rights to privacy and freedom from exploitation and abuse. Although not formulated in the digital age, the provisions also apply to children's rights online. A crucial component of the CRC is that it demands that children's rights be considered holistically. In this regard, governments are obligated to take action in ensuring the safety and protection of every child in every aspect of their life.[126] There should be a balance between the rights of children to be protected and their right to education, participation, information, privacy and respect for their developing capacities and emerging autonomy.[127]

Four general principles have been identified by the UNCRC that inform the realisation of all other rights. These are non-discrimination, best interests of the child, survival and development, and child participation. These principles have relevance to children's rights to privacy, freedom from exploitation and abuse hence should be applied when addressing protection of children's rights online.

Right to privacy

Article 16 provides that no child shall be 'subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation'. The inclusion of 'correspondence' is of significance in the digital context as it implies that children's forms of communications, including through the internet, should not be interfered with unlawfully. This means that any instances permitting interference with a child's communication should be prescribed by law.[128] Regarding 'unlawful attacks on honour and reputation', the provision implies that there should be laws in place to protect children from conduct either

[125] United Nations Human Rights Office of the High Commissioner Status of ratification Interactive Dashboard<https://indicators.ohchr.org/ > accessed 21 October 2020.

[126] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (UNICEF 2012) 52 <www.unicef-irc.org/publications/652-child-safety-online-global-challenges-and-strategies-technical-report.html> accessed 13 September 2020.

[127] ibid.

[128] UNICEF, *Implementation handbook for the Convention on the Rights of the Child* (UNICEF: Atar Roto Presse 2007) 210.

verbally, orally or through the media which may have negative impacts on their reputation.[129] It is relevant to highlight that the UNCRC has raised concerns on the portrayal of children's individual and collective images by the media, which may have negative effects on children's reputation.[130]

Looking at the right to privacy online, this provision implies that states must ensure that internet service providers (ISPs) and online access services such as social networking sites, online gaming and internet café owners safeguard suitable levels of privacy for consumers including children.[131] The other implication is the obligation placed on states to ensure that children who are navigating the internet have adequate knowledge and guidance so that they can be able to safeguard their right to privacy efficiently online.

The draft General Comment 25 also notably protects children's right to privacy online. Some of the noteworthy provisions include the call for states to take legislative and other measures to ensure the protection of privacy of children by all organisations and environments that process their data.[132] Further, privacy and data protection laws should not limit children's other rights such as freedom of expression and protection rights.[133] Online surveillance of children shall respect children's right to privacy and should not be conducted without the consent of the child involved or the consent of a parent or guardian in respect of younger children.[134]

Exploitation and abuse

Article 19 requires state parties to take all 'appropriate legislative, administrative, social and educational measures' to ensure the protection of children from all forms of violence, or abuse, neglect, maltreatment or exploitation, including sexual abuse. The application of this right is not limited to abuses that are the result of conduct sanctioned by the state, nor does it limit its scope to certain manifestations of abuse.[135] States are obliged to protect children from exploitation committed in any sphere

[129] UNICEF, *Implementation handbook* (n 128) 211.
[130] UNCRC 'Report on the eleventh session' (22 March 1996) UN Doc CRC/C/50.
[131] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (n 126) 53.
[132] UNCRC Draft GC 25 (n 123) para 71.
[133] ibid para 75.
[134] ibid para 76.
[135] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (n 126) 53.

including the internet. Article 34 of the CRC reinforces this provision as it requires governments to take all appropriate steps to prevent, among other things, the enticement or compulsion of a child to take part in any illicit sexual activity, child prostitution and child pornography. As such, there are no limitations imposed on the terms of engagement. This implies that if the engagement takes place by electronic means, it too would be an infringement of the right.[136]

General Comment 13 affirms the scope of the provisions of article 19 to address violence through information communication technologies, including the sexual exploitation and abuse of children for production and dissemination of child abuse images, exposure of children to harmful content, bullying or grooming.[137]

The draft General Comment 25 further requires states to ensure that businesses meet their obligation to effectively protect children from all forms of online violence including cyber-bullying, online grooming, sexual exploitation and abuse.[138] Further, states should provide accessible, child-friendly and confidential online reporting and complaint mechanisms to enable individuals to report cases of online abuse.[139] States are also called upon to take a 'safety-by-design approach to anonymity to ensuring that anonymous practices are not routinely used to hide harmful behaviour', for instance cyberbullying or hate speech.[140]

The role of parents is also worth discussing when talking about children's rights in the CRC. Article 5(1) requires states to respect the responsibilities of parents, legal guardians or other legally responsible persons for a child and to provide guidance on the exercise of rights by a child in a manner consistent with the evolving capacities of the child. This means that adults must respect and promote children's development towards adulthood.[141] Due weight is given to the age and maturity of the child and in most instances, younger children need more guidance than older children.[142]

[136] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (n 126) 53.
[137] UNCRC 'General Comment 13 on the right of the child to freedom from all forms of violence' (18 April 2011) UN Doc CRC/C/GC/13.
[138] UNCRC Draft GC 25 (n 123) para 87.
[139] ibid para 88.
[140] ibid para 78.
[141] UNICEF, *Implementation handbook* (n 128) 77.
[142] ibid.

In the digital context, various measures can be employed by parents in monitoring children online. It is however critical to note that whilst the objective of parental supervision is undoubtedly legitimate as children are protected from online risks, a clear interference with children's privacy,[143] freedom of expression, access to information, participation and development of digital literacy is presented by parental controls.[144] The reliance on the involvement of parents does not consider the empirical evidence that shows that children are mindful of the privacy threats to which they are exposed online, in as much as their parents are.[145] Moreover, as indicated in the previous chapter, threats to children's privacy may also emanate from parents who share information about their children online as most children are not able to object to what their parents share online about them.[146] As such, in addressing the tension between parental supervision and children's right to privacy and engagement with the cyberspace, due deliberation needs to be given to the importance of the internet as a resource and a means of increasing and strengthening children's capacities, and their evolving capacities.[147]

3.2.2 Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography

The OPSC seeks to strengthen the provisions of the CRC in various ways relevant to online and offline sexual exploitation of children. Of particular relevance for children who are at risk of different forms of online exploitation is an obligation imposed on states to keep up with new technologies to ensure protection of children's rights.[148] Article 1 obliges states to prohibit the sale of children, child prostitution and child pornography. In terms of article 3(1)(c), simple possession of

[143] UNICEF, 'Children's Rights and Business in a Digital World: Privacy, protection of personal information and reputation' (Discussion Paper Series, UNICEF 2017) 17 <www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf> accessed 12 September 2020.

[144] MV Cunha, 'Child Privacy in the Age of the Web 2.0 and 3.0: Challenges and opportunities for policy' (Innocenti Discussion Paper 2017-03 UNICEF 2017) 14 <www.unicef-irc.org/publications/926-child-privacy-in-the-age-of-web-20-and-30-challenges-and-opportunities-for-policy.html> accessed 21 August 2020.

[145] L Jasmontaite and De Hert, 'The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet' (2015) 5 International Data Privacy 7.

[146] Cunha (n 144) 14-15.

[147] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (n 126) 53.

[148] ibid 54.

child pornography should be criminalised regardless of the intent to distribute. States are required to include in their criminal or penal laws child sexual exploitation offences, whether committed inside or outside their boarders in terms of article 3(1).

Article 3(4) addresses the liability of legal persons and encourages states to establish such liability for offences specific to child pornography. This article reflects the notion that a comprehensive approach requires industry involvement.[149] Further, in terms of article 9(1), states should 'adopt or strengthen, implement and disseminate provisions to prevent sexual crimes against children,' which also includes information on online safety.

3.2.3 Council of Europe's Convention on Cybercrime

The Cybercrime Convention was established in the anticipation of realising a cooperative and uniform approach to the prosecution of cybercrimes. This was as a result of developments in technology that have enabled perpetrators of cybercrime to be in different jurisdictions from the victims.[150] Of particular relevance is article 9(1) which criminalises child pornography and article 12(1) that addresses corporate liability for a criminal offence established in accordance with the convention.

3.2.4 Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

The Child Protection Convention focuses on ensuring that the best interests of children is upheld through prevention of exploitation and abuse, protection and assistance for survivors of abuse, retribution of offenders and promotion of national and international law enforcement. It criminalises child pornography in article 20 and solicitation of children for sexual purposes in article 23. In article 26(1), state parties should enact legislation to ensure that a legal person can be held accountable for an offence created in the convention.

[149] International Centre for Missing and Exploited Children, 'Child Pornography: Model Legislation & Global Review' (International Centre for Missing and Exploited Children 2012) 10 <www.icmec.org/wp-content/uploads/2015/10/7th-Edition-EN.pdf> accessed 12 October 2020.

[150] ibid.

3.2.5 International Telecommunications Unit Resolution 179

The ITU whose membership is open to all UN members adopted Resolution 179 which provides for online child protection. The resolution among other things calls upon member states to raise awareness on online risks that may be encountered by children, establish frameworks for child protection online, and support the collection and analysis of data and statistics on child online protection which are key in designing and implementing public policies.[151] The ITU has further developed guidelines for online child protection which can serve as guidelines for stakeholders on how they can contribute to the development of a safe online space for children.[152]

3.2.6 UN Guiding Principles on Business and Human Rights

The Guiding Principles call upon all industries to adopt suitable strategies and processes to meet their obligation to respect human rights. Private sector players, including the information and communications technology (ICT) industry, also have an important role to play in fulfilling children's rights online.[153] Companies are required to take appropriate actions to detect, prevent, alleviate, and where suitable, redress possible and actual negative effects on children's rights in the online environment.[154]

Building on the Guiding Principles, the Children's Rights and Business Principles[155] call on industries to meet their responsibility to fulfil children's rights by circumventing any adverse effects associated to their work, products or services. In protecting children's rights online, a careful balance needs to be struck by businesses between children's protection and participation rights. Businesses should thus ensure that strategies to protect children online are targeted and are not unreasonably restraining, either for children or other internet users.[156]

[151] ITU Resolution (n 121).
[152] ibid.
[153] UNICEF, 'Children's Rights and the Internet: From Guidelines to Practice' (UNICEF 2016) 8 <www.unicef.org/csr/files/Childrens_Rights_and_the_Internet_Guidelines_to_Practice_Guardian_Sustainble_Business_English.pdf> accessed 21 October 2020.
[154] ibid.
[155] UNICEF, UN Global Compact and Save the Children, 'Children's Rights and Business Principles' (2012) <www.unicef.org/documents/childrens-rights-and-business-principles> accessed 21 October 2020.
[156] UNICEF, 'Children's Rights and the Internet: From Guidelines to Practice' (n 153).

Children should be given special attention as a vulnerable group with regards to data privacy and protection hence businesses have a duty to respect children's rights, even where national legislation is not yet in line with international standards.[157] Furthermore, companies should have reporting mechanisms to enable victims to report abuses. Combined with internal processes to address adverse impacts, reporting mechanisms should ensure companies have functioning structures to enable children to have appropriate redress in the event of infringement of their rights online.[158] These must be 'legitimate, accessible, predictable, equitable, transparent, rights-compatible, a source of continuous learning, and based on engagement and dialogue'.[159]

3.3 Regional legal framework

The main instruments that address children's rights are the African Charter on the Rights and Welfare of the Child (ACRWC)[160] and the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).[161] The Southern African Development Committee (SADC) has also adopted a model law on data protection and ICT that provides a valuable framework for SADC countries desiring to adopt legislation in this area.[162]

3.3.1 African Charter on the Rights and Welfare of the Child

The ACRWC incorporates the universalist outlook of the CRC but at the same time applies the African cultural context to its conceptions.[163] Emphasis is on that:

> The concept of the rights and welfare of the child should be inspired and characterised by the virtues of the African cultural heritage, the historical background and the values of the African civilisation.[164]

[157] UNICEF, 'Children's Rights and the Internet: From Guidelines to Practice' (n 153).
[158] ibid.
[159] UN Guiding Principles on Business and Human Rights (n 122) principle 31.
[160] African Charter on the Rights and Welfare of the Child (adopted 1 July 1990, entered into force 29 November 1999) CAB/LEG/24.9/49 (1990) (African Children's Charter).
[161] African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014)
[162] SADC Model Law on Data Protection (2013)
[163] SS Terblanche and N Mollema, 'Child Pornography in South Africa' (2011) 24 South African Journal of Criminal Justice 286.
[164] Preamble to the ACRWC.

Right to privacy

Article 10 protects children's right to privacy. It is important to note that the article provides that 'parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children'. This provision can be applied to children's privacy online and it implies that parents and guardians have a right to reasonably monitor and supervise children's online activities.

Freedom from exploitation and abuse

Article 16(1) requires state parties to adopt specific 'legislative, administrative, social and educational measures' to ensure the protection of children from all forms of 'torture, inhuman or degrading treatment and especially physical or mental injury or abuse, neglect or maltreatment including sexual abuse'. Further, article 27 places an obligation on state parties to protect the child from all forms of sexual exploitation and sexual abuse. In particular, state parties are required to prevent the use of children in pornographic activities, performances and materials. This is a noteworthy provision as it further protects children from sexual abuse and exploitation online in the form of child pornography.

It should be noted that the African Children's Charter also provides for the role of parents and guardians in upholding children's rights. Article 20(1) provides that 'parents or other persons responsible for the child shall have the primary responsibility for the upbringing and development the child'. This is a reinforcement of the role of parents alluded to in article 10 which provides that parents or guardians can exercise reasonable supervision on their child's privacy. This formulation is in line with key tenets of international standards to regulatory environments around children and digital media, that is, parents provide the necessary guidance and control over digital content in the first instance as opposed to state authorities or other regulatory agencies.

3.3.2 African Union Convention on Cyber Security and Personal Data Prevention

In terms of article 8(1) of the Malabo Convention, state parties should put in place legal frameworks aimed at strengthening fundamental rights and freedoms, especially protection of data and sanction any infringement of privacy. In terms of article 8(2), any form of data processing should respect fundamental rights and freedoms. The Malabo Convention however has no section addressing processing of data relating to children.

Protection of children from exploitation and abuse online is provided for in article 29(3)(1) which calls upon state parties to criminalise child pornography. Article 29(3) provides that:

> State parties shall take the necessary measures to ensure that, in case of conviction, national courts will give a ruling for confiscation of materials, equipment, instruments, computer program, and all other devices or data belonging to the convicted person and used to commit any of the offences mentioned in the Convention including child pornography.

The Malabo Convention is however not yet in force as it only has eight ratifications,[165] and requires ratification by 15 countries in terms of article 36.

3.3.3 Southern African Development Committee model law on data protection and information and communications technology

The model law protects privacy of children as it provides that the personal data of a child may be processed only subject to the provisions of article 37 of the model law, which provides that 'if a child is the data subject, his or her rights may be exercised by his or her parents or legal guardian'. If, however, in terms of national law, a child is able to provide consent individualistically according to his or her age and ability, this shall be allowed, in line with the key tenets of international standards that requires respecting the evolving capacities of children.

[165] Malabo Convention ratification list as at 18 June 2020 < https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf > accessed 21 October 2020.

3.4 National legal frameworks

International and regional treaty ratification[166]

Instrument	Status	
	Zimbabwe	**South Africa**
Convention on the Rights of the Child	Ratified	Ratified
Optional Protocol to the CRC on the sale of children, child prostitution and child pornography	Accession	Accession
European Union Convention on Cybercrime	No action	Signed
European Union Child Protection Convention	No action	No action
Malabo Convention	No action	No action
African Charter on the Rights and Welfare of the Child	Ratified	Ratified

As shown in the table above, Zimbabwe and South Africa are state parties to some international and regional instruments that protect children's rights. According to Akdeniz, the provision and harmonisation of the legal standards set out in these instruments by member states is a significant step towards mitigating online abuse of children.[167] Zimbabwe and South Africa thus have an obligation to ensure that the provisions of the instruments are domesticated in their laws.

3.4.1 Zimbabwe

Currently, in Zimbabwe, there are no specific laws that deal with data protection and online abuse of children as the Cybercrime Bill is not yet in force. As such, reference is made to the laws that provide for the protection of children's rights and general legislation that has an impact on internet usage.

[166] See treaty ratification status for ACRCW <https://au.int/sites/default/files/treaties/36804-sl-AFRICAN%20CHARTER%20ON%20THE%20RIGHTS%20AND%20WELFARE%20OF%20THE%20CHILD.pdf > accesed 21 October 2020 , CRC Status of ratification (n 125), EU Convention on Cybercrime Chart of signatures and ratifications of treaty 185 <www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185> accessed 21 October 2020, EU Child Protection Convention Chart of signatures and ratifications of treaty 201 <www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=201 > accessed 21 October 2020, Malabo Convention ratification list (ibid) and OPSC Status of ratification (n 125).

[167] Y Akdeniz, *Internet Child Pornography & the Law: National & International Responses* (Ashgate 2008) 13.

Constitution of Zimbabwe Act 20 of 2013

Section 57 provides that every person has the right to privacy and this includes privacy of communications. Section 81(1)(e) provides for the protection of children from economic and sexual exploitation and any form of abuse. The best interests of the child is the primary consideration in all issues affecting children in terms of section 81(2), in line with international standards. The rights provided in the constitution also apply to the online environment.

Interception of Communications Act 6 of 2007

This act provides for the lawful interception and monitoring of communications of any form of transmission in Zimbabwe. Section 3 makes unlawful interception of communication an offence. Although the act does not explicitly mention children, the provisions can be used to protect children from unlawful interception of their communications. The act has been criticised for encroaching on communication rights and freedoms through unregulated surveillance, potentially undermining the implementation of just and fair internet governance regime thus also infringing upon children's participation rights online.

Freedom of Information Act 1 of 2020

The act regulates the procedure for citizens to access information held by public institutions. Section 21(1) which prohibits information officers from releasing information relating to a third party if release of that information would involve the disclosure of personal and confidential information about the third party. Section 22(1) further states that 'trade secrets, financial or commercial information, or information of a third party, or information supplied in confidence by a third party should not be divulged'. This protects information belonging to third parties. There are however exceptions to this provision and this can be for instance where the third party has consented to their information being divulged or the disclosure is necessary to facilitate accountability, or revealing misconduct or deception. The provisions of the act are however silent about information concerning children.

Consumer Protection Act 5 of 2019

The act which also applies to electronic transactions may be used in relation to protection of personal information. Section 48(1) provides that any person who receives any confidential information pertaining

to a customer or prospective customer has a duty to protect such information. Release of confidential information requires the consent of the customer or prospective customer in terms of section 48(1)(b). Section 78 makes it an offence to disclose confidential information obtained unless such disclosure is for the purpose of compliance with or administration of the act or for the purpose of administrative justice. Employees and employers are jointly and severally liable for contravention of the provisions including the confidentiality provisions in terms of section 81. This is a good step considering the duty of businesses to ensure the safety of consumer's rights including the right to privacy. Although it can be said that this act protects the right to privacy through the prohibition of disclosure of consumers' information and holding employers and employees liable for breach, the challenge is that it does not make explicit reference to children who can be consumers online.

Censorship and Entertainment Controls Act 22 of 2001

Section 13 prohibits importation, production and dissemination of undesirable publications, pictures, statues and records. The act is however not explicit on exposure to inappropriate content by children or child pornography. One may even wonder what the meaning of 'undesirable' is as the definition is not provided. Concerns have also been raised that the act, through the use of the term 'import', is concerned with the physical bringing of materials into Zimbabwe that is considered unsafe.[168] This has been viewed as problematic in the digital era as the definition excludes electronic importation in the form of access to the internet.[169] As such, the act does not explicitly protect children from online exploitation and abuse. Another challenge is that the act does not compel ISPs and internet café owners to restrict access to harmful sites,[170] which increases the vulnerability of children to being exposed to inappropriate content online. This is against international standards that call upon states to ensure that businesses safeguard children's rights online.

[168] O Saki, *Internet governance in Zimbabwe: An analysis of legislation that has an impact on the use of the internet* (MISA Zimbabwe 2016) 13.
[169] ibid.
[170] ibid.

Children's Act 23 of 2001

The Children's Act which provides for the protection and supervision of the welfare of children fails to make provision for protection of children's right to privacy. Section 7 which provides for the prevention of neglect, ill-treatment and exploitation of children only applies to parents or guardians and fails to address ill-treatment and exploitation of treatment in the online environment. Section 8(2) however provides that:

> Any person who causes or conduces to the seduction, abduction or prostitution of a child or young person or the commission by a child or young person of immoral acts shall be guilty of an offence.

This provision can be used in relation to child pornography and grooming although it does not specifically make reference to such.

Criminal Law (Codification and Reform) Act 23 of 2004

Section 81 prohibits soliciting of another person for the purposes of prostitution and this involves publication of the solicitation in any printed or electronic platform for reception by the public. Although this provision can be used in cases of child pornography meant to promote child prostitution in the online environment, it is not comprehensive and does not make specific reference to children.

Section 95 provides that 'any person who seriously impairs the dignity of another or seriously invades the privacy of another person whether by words or conduct shall be guilty of criminal insult'. The provision also refers to instances of intentional invasion of privacy or where the conduct of the offender was reckless such that he or she should have foreseen the real risk or possibility that such words or conduct could have resulted in such effect.[171] This does not preclude cases of revenge pornography where individuals share nude images and when relations sour, the aggrieved party shares the pictures online. In such instances, the subject of the image would not have consented to the whole world having a glimpse of their private life.[172] The section, although silent about children, can be used in cases of revenge pornography which may also be a result of children's conduct online.

Although section 162 provides for computer related crimes, this relates to the unauthorised use or access to computers and does not address data protection or online exploitation.

[171] MISA Zimbabwe, 'Online abuse and the law' *Zimbabwe Mail* (Harare, 6 November 2019).
[172] ibid.

Sexual Offences Act 8 of 2001

The act focuses on aspects of extra-marital sexual intercourse with young persons, rape, sodomy and indecent acts. Young persons are defined as persons below the age of 16. This is problematic as the definition of a child in the constitution is a person below the age of 18. One can therefore argue that not all children are protected from sexual exploitation. The act criminalises solicitation of another person for immoral actions in section 9(1)(c), procuring a person to have sexual intercourse in section 11 and coercing a person to have extra-marital intercourse in section 12. Although the provisions can be used to protect children, they do not explicitly address issues of child pornography and grooming.

Cyber-Security and Data Protection Bill

The bill aims to address cybercrime and provide for data privacy and protection with due regard to the rights enshrined in the constitution. Clause 13 prohibits the processing of sensitive personal information without the data subject's consent. Clause 26 provides that where the data subject is a child, his or her rights may be exercised by his or her parents or legal guardian. The bill thus protects children's right to privacy by prohibiting the processing of their personal information without parental consent, although the provision can be expanded.

The bill further has a section on 'Offences against Children.' Clause 165 criminalises child pornography whilst clause 165A makes it an offence to expose children to pornography. Whilst this can be hailed as a progressive provision as it protects children from exploitation and abuse online, the bill has been criticised for its definition of child pornography. Child pornography is defined as:

> Any representation through publication, exhibition, cinematography, electronic means or any other means whatsoever, of a child engaged in real or simulated explicit sexual activity, or any representation of the sexual parts of a child for primarily sexual purposes.

This definition appears incomplete and insufficient for purposes of curtailing such criminal behaviour. Further, sexually explicit activity is an ambiguous term that needs further definition.

The bill can also be criticised for failing to protect children from all forms of online exploitation. It is surprising that the drafters enacted a section for offences against children which only focuses on child pornography yet children are susceptible to other abuses such as

cyberbullying, cyber grooming, exposure to inappropriate content and threats to their privacy and unauthorised use of children's information. Although one may argue that the bill criminalises cyberbullying, revenge pornography and identity theft under clause 164B, 164E and 164G respectively, these are however general provisions that are silent about children. Children deserve specific protection hence these should have been explicitly provided under the section addressing offences against children.

One step forward

In 2019, Zimbabwe launched the Zimbabwe Child Online Protection Task Force under the auspices of the Ministry of Information and Communication Technology, Postal and Courier Services. The task force is working with Interpol to investigate crimes committed inside and outside borders in efforts to protect children against cybercrime. However, no cases have been dealt with yet. Furthermore, the Postal and Telecommunication Regulatory Authority of Zimbabwe has developed guidelines on online safety for children,[173] in line with international obligations placed on states to ensure that children have adequate information and guidance to enable them to protect themselves effectively online. Various non-governmental and inter-governmental organisations such as Childline and UNICEF are also working with the government to raise awareness on child online safety.

3.4.2 South Africa

South Africa, unlike Zimbabwe, has made progress in terms of aligning its legislation with international standards on the protection of children's rights online.

Constitution of South Africa 108 of 1996

The right to privacy is protected in section 14 and of particular relevance to ICTs is protection of privacy of communications. Section 28 which addresses children's rights provides for the protection of children from maltreatment, neglect, abuse or degradation.[174] In terms of section

[173] POTRAZ, 'Child Online Protection Guidelines for Children' (POTRAZ 2015) <www.potraz.gov.zw/wp-content/uploads/2015/05/POTRAZ_COP.pdf> accessed 13 September 2020.

[174] Constitution of South Africa 108 of 1996, s 28(1)(d).

28(2), the best interests of the child is the primary consideration in all issues affecting children. The provisions of the constitution can be used to protect children's rights in the digital sphere.

Protection of Personal Information Act 4 of 2013

This is the principal data protection legislation in South Africa. Some of its aims are to promote the protection of personal information processed by public and private bodies. The act significantly has a section that explicitly addresses the processing of data relating to children. In terms of section 34, the processing of personal information concerning a child is prohibited unless if consent has been obtained from a competent person, that is, any person who has legal capacity to consent to any action or decision being taken in respect of any matter concerning a child. This can be hailed as a positive step towards protection of children's right to privacy.

Regulation of Interception of Communications and Provision of Communication-related information Act 70 of 2002

Section 2 of the act prohibits the interception of communications. This is buttressed by section 49 which makes the unlawful interception of communications an offence. There are exceptions however to the interception of communications and examples are where an interception direction has been obtained from a judge,[175] and when consent of the party involved has been obtained.[176] In terms of section 42(1), disclosure of information obtained under the exceptions provided for is prohibited. The provisions of this act, although not explicit about children, can also be used to prohibit the unlawful interception of communications relating to children.

Electronic Communications Transaction Act 25 of 2002

The act prohibits unauthorised access to, interception of or interference with the data of individuals.[177] In terms of section 81(2), 'any person who with intent, accesses or intercepts any data without authority or permission is guilty of an offence'. The act can be used to protect children although it does not make specific reference to children.

[175] Regulation of Interception of Communications and Provision of Communication-related information Act 70 of 2002, s 16(4).
[176] Interception of Communications Act 6 of 2007, s 5.
[177] Electronic Communications Transaction Act 25 of 2002, s 86.

Consumer Protection Act 68 of 2008

The act which also applies to electronic transactions has a section dealing with the privacy of consumers. Section 107 makes it an offence to disclose any personal or confidential information concerning the affairs of consumers. The act however does not explicitly provide for disclosure of personal information relating to children although the provisions can be used to protect children as well.

Children's Act 38 of 2005

The Children's Act augments children's basic rights by providing a legal definition of abuse and the procedures required to act in the best interests of the child and provide them with care and protection. In the definition of abuse in section 1, abuse includes sexual abuse, bullying and exposing or subjecting a child to behaviour that may be harmful to him or her. Commercial sexual exploitation on the other hand is defined as procurement of a child to perform sexual activities for financial or other reward and this includes prostitution and pornography. The forms of abuse defined in the act can be deduced in terms of harms perpetrated on the internet although this is not explicitly provided for.

Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007

The Criminal Law (Sexual Offences and Related Matters) Amendment Act is a significant step towards protecting children from sexual exploitation online in line with international standards that call upon states to keep current with emerging technologies. The act creates new offences such as child pornography and grooming. Of particular importance is the assertion of the drafters that despite the similarity of these offences to those created in respect of adults, the aim of creating the crimes specific to children is to address the particular vulnerability of children in respect of sexual exploitation or abuse.

Section 10 criminalises exposure or display of or causing exposure or display of child pornography to adults. Section 19 on the other hand criminalises exposure or display of child pornography to children. Using children for pornography or benefitting from child pornography is also an offence. The act goes on to further criminalise sexual exploitation of children for financial or other reward and grooming of children in terms of sections 17 and 18 respectively. The use of children for or benefitting from child pornography is a crime under section 20 of the act.

Section 42(1) provides for the establishment of a National Register for Sex Offenders containing details of individuals convicted of any sexual offence against a child. A sex offenders register is necessary to monitor sex offenders upon discharge from prison to ensure that they are not employed in institutions where they have to interact with children; and to keep them under monitoring to try to stop them from re-offending.[178]

The provisions of the act thus go far in protecting children's right to freedom from online exploitation and abuse. This is in line with the provisions of the OPSC which requires states to include in their criminal or penal laws child sexual exploitation offences.

It has however been argued that the offences created by the sexual offences legislation largely overlap with those created in the Films and Publications Act.[179] This may cause problems should there be a need to institute prosecution for offences such as displaying child pornography to another person or the creation of child pornography. The act has also been criticised for not attaching penalties to offences which may lead to inconsistencies on the sentences imposed by judicial officers should one be convicted of an offence under the act.

Protection from Harassment Act 17 of 2011

In the act, harassment also includes 'engaging in verbal, electronic or any other communication aimed at the complainant, by any means', regardless of whether the conversation takes place or not.[180] In terms of section 2, one can apply for a protection order against harassment, including online harassment. The act further provides in section 2(4) that 'any child, or person on behalf of a child, may apply to the court for a protection order without the assistance of a parent, guardian or any other person'. This ensures that in cases of harassment, particularly online, children can combat harassment, without parental consent.

In terms of section 4(1), if the court is convinced that a protection order has to be issued in respect of online harassment and the identity or address of the respondent is unknown, it may direct an electronic service provider to furnish the court with particulars such as the identity number from where the harassing electronic communication originated,

[178] G Feltoe, 'Strengthening our law on child sexual abuse' (2017) 1 Zimbabwe Electronic Law Journal 6.
[179] Terblanche and Mollema (n 163) 303-04.
[180] Protection from Harassment Act 17 of 2011, s 5(1)(a).

details of the respondent and any information that can assist the court in identifying the offender or the service provider which provides a service to the offender. This is a valuable addition in respect of cyberbullying cases that are increasing.

Films and Publications Amendment Act 11 of 2019

The Films and Publications Act as amended is progressive legislation in the protection of some of children's rights online as it expansively addresses the issue of child pornography to bring South Africa in line with its international obligations under the OPSC.

Section 18G(1) states that 'no person may create, produce or distribute in any medium, including the internet, and social media any films or photographs depicting sexual violence and violence against children'. This prohibition applies regardless of whether the victim consented to the original creation of such photograph or film.

Section 24(A)(4)(a) and section 24(3)(j) make it an offence to knowingly or negligently grant children access to a film, game or publication rated 'X18'. This also applies in granting children access to scenes of explicit sexual conduct. In terms of section 24, registered film or game distributors may, subject to an exemption being granted by the South African Film and Publication Board, distribute a film or game classified as 'X18' online, subject to the conditions such as ensuring that children would not be able to access such a film or game online.

Section 24B criminalises child pornography. The section has however been criticised in that it does not simply criminalise possession or distribution of child pornography as defined in the act. The section criminalises 'possession, distribution of any film, game or publication which contains depictions, descriptions or scenes of child pornography'. This is problematic because the act defines child pornography as 'any image or description of all kinds of sexual activities involving children'. Surprisingly, the act reverts to mentioning films, games and publications with scenes of child pornography. On the face of it this appears to involve a backward step to a definition that includes visual representations only. Taken literally, section 24B provides that:

> Any film, game or publication which contains depictions, descriptions or scenes of any image, however created, or any description of a person, real or simulated, who is or who is depicted, made to appear, look like, represented or described as being under the age of 18 years, engaged in sexual conduct.

This does not make sense and might pose challenges for the courts in interpreting section 24B.

ISPs have a role to play in terms of online safety of children. In terms of section 24C(2), ISPs must take reasonable steps to ensure that their services are not being used for committing offences against children. Further, ISPs must display safety messages for children,[181] provide mechanisms for children to report suspicious behaviour[182] and report commission of offences against children.[183]

The Film and Publications Act has been criticised as sharing of sexual images amongst children can result in prosecution for the production and distribution of child pornography. Such measures have been said to be counterproductive and against the spirit of the CRC as they unreasonably criminalise children's conduct without providing mitigating or alternative measures for them.[184] Additionally, extensive measures that do not consider age appropriateness, intention or consent can be equally damaging. Despite creating a risk that children will be placed on the sexual offenders register and branded as criminals, there is a possibility of the creation of an atmosphere of reluctance to report cases of online abuse for fear of prosecution.[185]

The provisions of the act can however be hailed as progressive as they not only seek to combat child pornography but also exposure of children to inappropriate content online. Further, the act provides for the role of businesses in keeping children safe online which is in line with international standards that call for business to protect children from online violence.

Cybercrime Bill

The bill, which is not yet in force, protects the right to privacy by making the unlawful interception of data an offence in clause 3. Although silent about children, this provision can be used to address interception of data with regards to children. With regards to online abuse, clause 14 makes the unlawful distribution of data messages which incite damage to property or violence an offence whilst clause

[181] Films and Publications Amendment Act 11 of 2019, s 24C(2)(b).
[182] ibid s 24C(2)(c).
[183] ibid s 24C(2)(d).
[184] J Byrne and P Burton, 'Children as Internet users: how can evidence better inform policy debate?' (2017) 2 Journal of Cyber Policy 40.
[185] ibid.

15 addresses distribution of data messages which threaten persons with damage to property. The distribution of data messages of intimate images of another person without their consent is an offence. These provisions are however silent about children.

In terms of clause 21, ISPs can be directed to furnish the court with further particulars if the identity of the perpetrator is not known. The bill further seeks to make amendments to the Sexual Offences Act and the Films and Publications Act with regards to child pornography. The bill can be criticised for not adequately covering all aspects of child online abuse such as cyberbullying and exposure to harmful content.

Another step forward

Significantly, the Film and Publication Board and its Pro-Child Website gives citizens the opportunity to report and expose cases of child sexual abuse through images that appear on the internet by using a hotline number given. This step makes South Africa the first African country to join a global umbrella body of internet hotlines established to combat child pornography.[186]

The Press Council and the Interactive Advertising Bureau of South Africa has also adopted a Code of Conduct for South Africa Print and Online Media. The code protects children as the media is required not to publish child pornography and avoid sharing violent, graphic content or explicit sex unless there is a warning that such content is graphic and inappropriate for certain audiences such as children. This ensures that children are protected from exposure to age inappropriate content.

South African courts have also dealt with cases of sexual exploitation of children in the online environment. This is an indication of enforcement of the law through the prosecution of offenders. In *S v Stevens*,[187] the accused was convicted for contravening sections 27(1)(a)(i) and (ii) of the Films and Publication Act – creating and possession of child pornography. He was sentenced to eight years imprisonment, with three years suspended and upon appeal the sentence he was sentenced to six years, with two years suspended. In *S v Kleinhas,*[188] a 74 year businessman was convicted for contravening the provisions of the Sexual Offences Act relating to the manufacture of child pornography,

[186] Terblanche and Mollema (n 163) 307.
[187] 2007 JDR 0637 (E).
[188] [2014] 2 SACR.

sexual assault and sexual grooming related to three minors he had confronted over a period of four years. He was sentenced to 15 years in prison and upon appeal the sentence was reduced to four years. Lastly, in *S v William Alexander Beale,*[189] an online child pornography website was discovered wherein the members engaged in peer to peer sharing of child pornographic material. One of the members gained access to the network from South Africa. He was sentenced to 15 years imprisonment and his name was recorded in the National Register for Sexual Offenders. On appeal, the sentence was reduced to ten years' imprisonment.

An analysis of the national legal frameworks indicates that at national level, both Zimbabwe and South Africa have ratified the CRC, ACRWC and made accessions to the OPSC. South Africa has taken a step further and signed the EU Convention on Cybercrime. The two countries have not however ratified the Malabo Convention nor signed the Child Protection Convention.

As required by international law, both countries have taken steps to enact legislation that protects children's rights in the digital age. Various organisations have also been working with government departments to raise awareness on online safety which is in line with international standards that require states to disseminate information to prevent online exploitation of children. Both countries have pending Cybercrime Bills that address some aspects of privacy and online child sexual exploitation.

Zimbabwe is lagging behind in terms of amending its legislation to incorporate aspects of online violence. The country does not have specific legislation dealing with data protection as the Cybercrime Bill is not yet in force. As such, reference is made to legislation that has an impact on the use of the internet, of which the legislation does not explicitly address children's privacy. The Criminal Law Code and the Sexual Offences Act further do not adequately address aspects of online exploitation and abuse of children such as child pornography, grooming and exposure of children to harmful content.

South Africa on the other hand has been progressive as there has been amendment of legislation to incorporate provisions relating to protecting children's rights online. The Protection of Personal

[189] Case no A283/18 (3 May 2019).

Information Act explicitly provides for the protection of children's data thereby protecting children's rights to privacy, although there is room for the provisions to be comprehensive. The Films and Publications Act, the Protection from Harassment Act and the Sexual Offences Act protect children from online exploitation and abuse which is a positive step, although there are a few gaps. The country has also prosecuted offenders for online exploitation of children, an indication of implementation of some of the laws that protect children's rights online.

3.5 Conclusion

Various steps have been taken at international and regional level to protect children's rights to privacy and freedom from online exploitation and abuse. At national level, the legal framework of Zimbabwe does not adequately protect children's rights to privacy and freedom from exploitation and abuse due to the lack of amendment of the legislation to apply in the digital context and the Cybercrime Bill which is meant to address some of the gaps in legislation is long overdue and not yet in force. South Africa on the other hand has made progress in terms of amending its legislation in order to protect children's rights in the digital environment although there is room for improvement. Best practices can be drawn from other jurisdictions that have made progress regarding protection of children's rights to privacy and freedom from online exploitation and abuse. The next chapter therefore discusses best practices relating to children's rights online that can be useful for law reform in South Africa and Zimbabwe.

4.

BEST PRACTICES FROM OTHER JURISDICTIONS

4.1 Introduction

The previous chapter demonstrated the need for law reform and amendment to the existing laws in South Africa and Zimbabwe for the legislation to adequately protect children's rights to privacy and freedom from online exploitation and abuse. In formulating or reforming legislation, sometimes it is useful to draw lessons from other jurisdictions although the blanket transposition of the law should be avoided. This chapter explores the legal frameworks on protection of children's rights online from other jurisdictions in order to draw best practices. The European Union (EU) regime on data protection, particularly the General Data Protection Regulation (GDPR)[190] and the legal framework of the United States of America (USA) particularly the United States Code (USC)[191] and the Children's Internet Protection Act (CIPA)[192] have been selected as comparators. The chapter begins by justifying the selection of the specific jurisdictions which is followed by a discussion of the legislation-focus being on the additional, child specific considerations. Insights will be drawn from the regimes to inform suggested reforms to the online protection of children framework.

[190] European Union General Data Protection Regulation (GDPR).
[191] United States Code (USC) (1994) <www.govinfo.gov/help/uscode#:~:text=The%20United%20States%20Code%2C%20is,was%20first%20published%20in%201926> accessed 12 October 2020.
[192] Children's Internet Protection Act 2000 (CIPA).

4.2 Rationale for selected legal regimes

The EU has one of the most broad data privacy protection frameworks globally and is regarded as a pacesetter and catalyst of data privacy protection laws.[193] The EU legal regime is hinged on three main factors: it is human rights centred,[194] it is one of the most comprehensive data privacy protection regimes and it specifically addresses current and anticipated challenges posed by technologies.[195] Further, the framework explicitly provides for the protection of children's data and introduces new requirements for the online protection of children's personal data.[196]

The USA on the other hand has enacted legislation that comprehensively addresses online exploitation and abuse of children, with additional protections offered to children. Both the EU and USA have been considered as jurisdictions that are in line with international standards in efforts to address online exploitation of children and signify a 'pre-eminent model of a political and moral accord to protect children from abusive adult practices, supported by a vigorous criminal legal and policy framework'.[197]

[193] AB Makulilo, 'Privacy and data protection in Africa: A state of the art' (2012) 2(3) International Data Privacy Law 163, 176.

[194] P Schwartz and KN Peifer, 'Transatlantic data privacy law' (2017) 106(1) The George Town Law Journal 123.

[195] CJ Hoofnagle, B Van Der Sloot and FZ Borgesius, 'The European Union General Data Protection Regulation: what it is and what it means' (2016) 28(1) Information & Communications Technology Law 65, 65-67.

[196] Information Commissioner's Office (ICO), 'Children and the GDPR' (*ICO*, 2018) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/> accessed 12 October 2020.

[197] M Bulger and others, 'Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online' (2017) 19 Sarah and George Journals 7.

4.3 The European Union legal regime

4.3.1 General Data Protection Regulation

This is a regulation in EU law on data protection and privacy. It also addresses the transfer of personal data. The GDPR replaced the Data Protection Directive and became effective in 2018.[198] The GDPR has provisions that precisely address children's right to privacy online and this is a welcome innovation. The fact that the GDPR recognised that children deserve special protection due to their vulnerability should be noteworthy.[199]

Conditions applicable to child's consent in relation to information society services

Article 8(1) provides that in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is aged 16. Where the child is below 16 years, parental consent is required. Such consent is however not required in the context of preventive or counselling services offered directly to a child.[200] Of particular significance is that the controller is required to take reasonable measures to verify that consent is given by the parent or guardian, taking into consideration available technology.[201] This is reinforced by recital 38 of the GDPR which states that children deserve 'specific protection with regards to their personal data, as they may be less aware of the risks, consequences and their rights in relation to the processing of personal data'. The high standard of consent set by the provisions of the GDPR are significant as they protect children's right to privacy online.

[198] EUR-Lex Access to European Union Law, 'The general data protection regulation applies in all Member States from 25 May 2018' (*EUR-Lex*, 24 May 2018) <https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html#:~:text=Share-,The%20general%20data%20protection%20regulation%20applies%20in%20all%20Member%20States,Directive%2095%2F46%2FEC> accessed 12 October 2020.

[199] D Krivokapić and J Adamović, 'Impact of general data protection regulation on children's rights in digital environment' (2016) 205-06 <www.researchgate.net/publication/312355507_Impact_of_general_data_protection_regulation_on_children's_rights_in_digital_environment> accessed 12 October 2020.

[200] GDPR, recital 38.

[201] ibid art 8(1)(2).

Transparent information, communication and modalities for the exercise of the rights of the data subject

Article 12 requires the controller to take suitable measures to provide any information relating to processing of data in a concise, transparent, understandable and easily accessible form, particularly any information specifically addressed to a child. This is bolstered by recital 58 which provides that the requirement is in line with the principle of transparency. This is of particular relevance in situations where technological complexities may make it difficult for one to understand the circumstances under which their personal data is being collected.[202] Considering the specific protection deserved by children, where the processing is related to a child, any information and communication should be in a language that can be easily understood by the child. This provision is significant, given the manner in which children use the internet sometimes, that is, when they are alone and not supervised, using personal phones and in some instances not understanding the language used by controllers.[203] This principle leads to a change in perception where children are not portrayed as a general group of consumers but a vulnerable group of internet users,[204] as reinforced by recital 75 of the GDPR.

Right to erasure

Article 17 requires companies to remove any personal data from any records which they no longer have a legitimate purpose for retaining. This can be where the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed,[205] where the personal data has been unlawfully processed[206] and where the personal data have been collected in relation to the offer of information society services directly to a child referred to in article 8(1).[207] This is expanded by the provision which stipulates that:

> Where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet, the data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.[208]

[202] Krivokapić and Adamović (n 199).
[203] ibid 216.
[204] ibid.
[205] GDPR, art 17(1)(a).
[206] ibid art 17(1)(d).
[207] ibid art 17(1)(f).
[208] ibid recital 65.

This provision ensures that data of children which is unlawfully processed or consent is mistakenly given is erased.

The European Court of Human Rights (the Court) has also dealt with a number of cases on the protection of privacy, including the protection of children's images. The cases are worth discussing as they relate to parental consent which applies both in the offline and online environment. In *Bogomolova v Russia,*[209] the Court dealt with a case concerning the use of a child's image without parental consent. The image was on the front page of a booklet meant to enlighten citizens about the local authorities' efforts to protect orphans and assist families wishing to adopt. The Court held that there had been a violation of the right to respect for private life as the image was used without parental consent. The Court held that the Russian courts erred in failing to assess whether consent for the 'publication' of the photograph was given by the applicant, concentrating instead on the fact that she had given authorisation for her child to be photographed. The Court also highlighted the false impressions and inferences which could be drawn from the context of the photograph, namely that the child was an orphan or had been abandoned, and the implication that could have on public perception of the relationship between the applicant and her son. Russia was ordered to pay €130 in respect of pecuniary damages and €7,500 in respect of non-pecuniary damages.

The case of *Hachette Filipacchi Associés v France,*[210] on the other hand indicates that children's privacy can be affected by the information published online about their parents. The case concerned the murder of a French prefect whereby a photograph of the corpse lying on the ground in a pool of blood, facing the camera, was published by a weekly magazine without the family's consent. The widow and her children approached the courts, alleging that their right to respect for their private life had been violated. The Court held, in particular, that the result of publication of the photograph, in a magazine with a very wide coverage, had been to increase the trauma experienced by the deceased's family, hence they were justified in arguing that their right to respect for their private life had been infringed.

[209] Application no 13812/09 (ECtHR, 20 June 2017).
[210] Application no 71111/01 (ECtHR, 14 June 2007).

Various countries in the EU have also passed legislation on data privacy which protects children's privacy online and have dealt with cases on the same. France for example has enacted legislation which prohibits the publication and distribution of another person's image without obtaining their consent. In terms of the penalties, offenders can face up to one year in prison or a fine of €45,000. This provision also applies to parents posting pictures of their children on social media.[211]

In the Netherlands, a woman was ordered by the courts to remove photos of her grandchildren from social media as she had posted them without their mother's consent. This was in terms of article 5 of the Dutch Act implementing the GDPR which provides that one must obtain consent from a legal guardian to process children's data and this includes posting pictures of a child below the age of sixteen years.[212] In Italy, the Rome courts held that a mother would have to pay a €10,000 fine if she posted pictures of her teenage son on Facebook without his consent. The issue was raised by the boy, aged 16, during divorce proceedings involving his parents. Under Italian law, the subject of the photo owns the copyright, rather than the person who took the photo.[213] As the teenager was featured in the pictures that were shared by his mother, the Court ruled that he could legally request their deletion from the social media platform. The mother was ordered to delete the photos and videos or face a fine.[214] This is an indication of the efforts that have been taken in the EU to protect children's information in the light of technological developments.

[211] G Moody, 'French Parents Face Fines, Lawsuits and Prison for Posting Pictures of Their Own Children Online' (*Tech Dirt*, 7 March 2016) <www.techdirt.com/articles/20160302/07480733781/french-parents-face-fines-lawsuits-prison-posting-pictures-their-own-children-online.shtml> accessed 4 October 2020.

[212] R Browne, 'Grandmother ordered to delete pictures of her grandkids on social media in EU privacy ruling' (*CNBC*, 22 May 2020) <www.cnbc.com/2020/05/22/gdpr-grandmother-ordered-to-delete-social-media-pictures-of-grandkids.html> accessed 4 October 2020.

[213] ibid

[214] ibid.

4.4 The United States of America legal regime

4.4.1 The United States Criminal Code

The USC is the codification by subject matter of the general and permanent laws of the USA. It is divided by broad subjects into different titles.[215] This includes titles that address sexual abuse and other abuse of children such as child pornography, online grooming, obscenity involving minors and bullying.

Child pornography

The USC has a clear and comprehensive definition of child pornography. Section 2256 of title 18 defines child pornography as 'any visual depiction of sexually explicit conduct involving a minor, that is, someone below the age of 16'. This includes photos, videos, generated images indistinguishable from an actual minor and images created, adapted or modified, but which appear to depict an identifiable, actual child. Further, undeveloped film, videotape and electronically stored data that can be converted into a visual image of child pornography are also considered illegal visual depictions.

Significantly, the legal meaning of sexually explicit conduct does not require that an image portray a child taking part in sexual activity.[216] As long as a photo of a naked child is sufficiently sexually suggestive, it may constitute child pornography.[217] Moreover, the age of consent for sexual activity in a given state is immaterial; any representation of a child below 18 years taking part in sexually explicit conduct is unlawful.[218] This ensures the protection of all children despite the fact that one has reached the age of consent and prevents offenders from exploiting children on the grounds that they have reached the age of consent.

The production, distribution, reception and possession of child pornography is prohibited in terms of sections 2251, 2252 and 2252A of title 18. Particularly, section 2251 prohibits the persuasion, inducement, enticement or coercion of a child to take part in sexually explicit conduct

[215] USC (n191).

[216] The US Department of Justice, 'Citizens' Guide to US Federal Law on Child Pornography' (*The US Department of Justice*, 28 May 2020) <www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography> accessed 12 October 2020.

[217] ibid.

[218] ibid.

for the production of child pornography. Attempt or conspiracy to commit a child pornography offence is also a crime.[219] In terms of section 2251A of title 18, parents, legal guardians or other persons in custody of a child are prohibited from buying, selling or transferring custody of that child for purposes of producing child pornography. Lastly, section 2260 of title 18 prohibits any individuals outside the USA to knowingly produce, receive, transport, ship or distribute child pornography with intent to import or transmit the visual depiction into the USA.

Child pornography is a serious offence and perpetrators face stiff penalties. In *US v James Snyder*,[220] the accused was convicted for producing, receiving, distributing and possessing child pornography. He was sentenced to 168 months of imprisonment followed by six years of supervised release. In *US v Donald Blakley*,[221] the accused was convicted for conspiracy to knowingly receive and distribute visual depictions of a minor engaged in sexually explicit conduct, 15 counts of knowingly receiving visual depictions of a minor engaged in sexually explicit conduct and possession of one or more electronically stored visual depictions of a minor engaged in sexually explicit conduct. He was sentenced to 87 months imprisonment.

The USC further criminalises the use of misleading domain names online with the intent to mislead a minor into viewing material that is harmful to minors under section 2252B(b) of title 18. Material that is harmful to minors is defined as 'any communication, consisting of nudity, sex, or excretion that predominantly appeals to the prurient interest of minors or is offensive to prevailing standards of suitable materials for minors'.[222]

Another important aspect is the obligation placed upon ISPs to report cases of child sexual exploitation to the Cyber Tip Line at the National Centre for Missing and Exploited Children under section 2258A(a)(1). Knowingly and wilfully failing to report sexual exploitation of children, while engaged to provide electronic communication service, is an offence attracting a fine of not more than $50,000.

[219] The US Department of Justice (n 216).
[220] [1999] 189 F 3d 640.
[221] [2005] 239 F 229.
[222] USC, s 2252B(d) title 18.

Online grooming

Online grooming is criminalised in section 2422(b) of title 18. Notably, the law has made it possible for perpetrators to be apprehended before the offline sexual abuse offence is committed. Police officers use covert sting operations whereby they enter online chat rooms, pretending to be children.[223] The police officers must only react to invitations and offers made to them as opposed to taking the initiative or approaching someone they suspect of paedophile activities.[224] The degree of protection offered to children is thus not only in theory but also in practise.

Obscenity involving minors

Section 1466A of title 18 makes it illegal for any person to knowingly produce, distribute, receive or possess with intent to transfer or distribute visual representations, such as drawings, cartoons or paintings that appear to depict minors engaged in sexually explicit conduct and are deemed obscene. Any individual who attempts or conspires to do so shall also be guilty of the offence.[225] Section 1470 of title 18 prohibits the transferring or attempting to transfer obscene matter using the US mail or any means of interstate or foreign commerce to a minor under 16 years. Further, it is illegal for an individual to knowingly use interactive computer services to display obscenity in a manner that makes it available to a minor less than 18 years,[226] and to knowingly make a commercial communication via the internet that includes obscenity and is available to any minor.[227] Convicted offenders generally face harsher statutory penalties than if the offence involved only adults. One can face up to ten years imprisonment for the offence.

Notably, section 16944(a) of title 42 requires the Attorney General to expand federal, state and local law enforcement and prosecutor training to help them respond to the threat of sex offenders using the internet and other technology to solicit children. The Attorney General is also required to deploy technology to all internet crimes against children task forces to track child exploitation. This ensures enforcement of the law.

[223] Childnet International, 'Online grooming and UK law' (*Childnet International*) <www.childnet.com/ufiles/online-grooming.pdf> accessed 12 October 2020)
[224] ibid.
[225] USC, s 1446A(2)(B) title 18.
[226] ibid s 223(d) title 47.
[227] ibid s 231 title 47.

Cyberbullying

Section 223(a)(1)(B) of title 47 makes it an offence to knowingly use a telecommunications device to make, create, solicit or initiate transmission of any comment, request, suggestion, proposal, image or other communication which is obscene or child pornography, knowing that the receiver of the communication is under 18 years of age. Further, harassing any person or repeatedly initiating communications with a telecommunications device to harass[228] are all offences punishable by fine and imprisonment for not more than two years, or both. This provision protects children from cyberbullying and harassment in the online environment.

4.4.2 Children's Internet Protection Act 2000

The main aim of the CIPA is to address concerns about children's access to obscene or harmful material over the internet specifically in schools or libraries.[229] Certain requirements are imposed on schools or libraries that receive discounts for internet access or internal connections through the E-rate programme – 'a program that makes certain communications services and products more affordable for eligible schools and libraries'.[230] Schools or libraries may not use funds received to purchase computers used to access the internet, and may not receive universal service discounts, except for telecommunications services, unless they enforce a policy that includes the operation of a technology protection measure that blocks or filters minors' internet access to visual depictions that are obscene, child pornography or harmful to minors; and that blocks or filters adults' internet access to visual depictions that are obscene or child pornography. The extension of child online protection to children in schools and libraries in the CIPA is worth noting hence South Africa and Zimbabwe can therefore draw lessons from the US regime in law reform.

[228] USC, s 223(a)(1)(E) title 47.

[229] Federal Communications Commission, 'Children's Internet Protection Act' (*Federal Communications Commission*, 30 December 2019) <www.fcc.gov/consumers/guides/childrens-internet-protection-act> accessed 11 October 2020.

[230] ibid.

4.5 Conclusion

In law reform, lessons can be drawn from other legal regimes that have made progress with regards to the protection of children's rights to privacy and freedom from online exploitation and abuse. The EU's GDPR contains detailed and explicit provisions on protection of children's personal information thereby protecting children's right to privacy. South Africa and Zimbabwe can draw lessons from the GDPR in reforming legal frameworks on data protection and privacy, particularly data of children. On the other hand, the USA has made notable improvements in the wide range protection of children from online exploitation and abuse through the provisions of the USC and CIPA. The provisions can be a trendsetter for law reform in South Africa and Zimbabwe in relation to the online exploitation and abuse of children. The next chapter provides a conclusion of the research and suggests recommendations based on the best practices of the legal regimes discussed.

5.

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The research assessed the extent to which children's rights to privacy and freedom from online exploitation and abuse are protected in South Africa and Zimbabwe. Whilst beneficial to some children, the internet has posed serious threats to children's privacy rights and opened avenues for the exploitation and abuse of children. The research established that the increase in internet access by children and the threats posed has created challenges to the existing legal frameworks on the protection of children's rights, thereby requiring South Africa and Zimbabwe to keep up with technological advancements and amend legislation to fit within the digital context. The legal framework of Zimbabwe does not adequately protect children's rights to privacy and freedom from online exploitation and abuse due to the lack of explicit laws regulating data privacy and lack of amendment of laws to incorporate provisions protecting children against online exploitation and abuse. The pending Cybercrime Bill which is meant to address some of the gaps has loopholes as it does not comprehensively address data protection of children and other forms of online exploitation and abuse such as use of children to produce child pornography, exploitation of children for financial gain, online grooming, exposure to harmful content and cyberbullying. South Africa on the other hand has made progress through the incorporation of provisions relating to the processing of children's data under the Protection of Personal Information Act thereby protecting children's privacy. The provisions can however be expanded to comprehensively address the protection of children's data. The provisions of the Sexual Offences Legislation and the Films and Publications Act also go a long way in protecting children from online exploitation and abuse as they

address issues of child pornography, exploitation of children for financial gain, online grooming and exposure of children to harmful content. The Protection of Harassment Act also protects children from online harassment. These laws can however be amended to comprehensively protect children. In law reform, South Africa and Zimbabwe can draw lessons from the EU through its adoption of the GDPR and the USA through its adoption of the USC and CIPA. In order to protect children's rights to privacy and freedom from online exploitation and abuse, the following recommendations are made.

5.2 Recommendations

5.2.1 Recommendations to states

1. South Africa and Zimbabwe should ratify the Malabo Convention and the Council of Europe Child Protection Convention. Zimbabwe should further ratify the Council of Europe Convention on Cybercrime.
2. Data privacy and protection laws in South Africa and Zimbabwe should be comprehensive, human rights centred and have explicit provisions regulating the processing of children's personal data. The laws should be clear on the duties of ISPs and websites in relation to processing of children's data and the penalties for breaches. Children should be consulted in the law reform process as they have a right to participate in matters involving them.
3. South Africa and Zimbabwe should amend legislation to incorporate provisions regulating internet usage in schools as was done in the USA.
4. The legislation in South Africa and Zimbabwe on online exploitation must clearly state that children are not criminally liable for online sexual offences. They should be regarded as victims and criminal responsibility must attach to adult offenders.[231]
5. South Africa and Zimbabwe should amend legislation to establish jurisdiction over crimes of online exploitation and abuse perpetrated

[231] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (UNICEF 2012) 78-79 <www.unicef-irc.org/publications/652-child-safety-online-global-challenges-and-strategies-technical-report.html> accessed 13 September 2020.

outside their borders when the victim is a national, and when the alleged perpetrator is a citizen or is a habitual resident in the territory, as required by the OPSC. Further, the legislation should enable individuals who habitually reside in the countries, but are not nationals, to be prosecuted for offences committed out of the country. This will ensure that offenders across the world are brought to justice.

6. South Africa and Zimbabwe should raise public awareness on the importance of children's digital rights and online safety in collaboration with businesses and civil society organisations. This includes providing parents, guardians, teachers and children with appropriate information on child online safety. The information should be presented in a way that reaches all children and speak to their different ages and evolving capacities. The use of local languages and braille is also encouraged.[232] Online safety should also be introduced to school curricula as this is an effective means of reaching out to many children. Alternative ways of reaching children out of school such as community outreaches and radio messages can be developed.[233]
7. South Africa and Zimbabwe should invest in capacity strengthening of professionals to tackle cases of online exploitation. This includes police officers, magistrates, judges, prosecutors, social workers and teachers. Police officers, in particular, should be supported with necessary infrastructure to identify and trace cases of online exploitation and abuse of children.
8. In South Africa, the offences created by the sexual offences legislation and section 24B of the Films and Publications Act should be accompanied by penalty clauses to avoid difficulties and inconsistencies when sentencing perpetrators.
9. Zimbabwe should incorporate provisions on child pornography, online grooming and exposure to harmful content in its sexual offences legislation, Criminal Code and Censorship and Controls Act. The definition of a child in the sexual offences legislation should also be in line with the constitution, that is, someone below the age of 18.

[232] UNICEF, *Child Safety Online Global Challenges and Strategies Technical Report* (n 231) 71.
[233] ibid.

10. The Cybercrime Bill of Zimbabwe should have a clear definition of what constitutes child pornography and sexually explicit conduct. The bill should state all parameters that may depict child pornography. Other aspects of online exploitation of children such as using children to produce pornography, exploitation of children for financial reward, grooming and exposure to harmful content, and cyberbullying should also be addressed.
11. Zimbabwe should have a sex offenders' register like South Africa and the legislation must make reporting cases of online exploitation should be compulsory.

5.2.2 Recommendations to businesses and ISPs

1. Businesses and ISPs should have transparent data collection methods and clear explanations on the purpose of collecting data. Privacy policies must be in clear and understandable language as provided for in recital 39 of the GDPR. This will ensure that children and their parents or guardians have a better appreciation of the reasons why data is collected and how it will be used.[234]
2. In setting rules on consent for the processing of children's personal data, businesses and ISPs should take into account the particular age of the child, evolving capacities and special susceptibilities. For example, parental consent may be a prerequisite for processing the personal data of children below a certain age (for example 13 years); beyond this age limit, parental consent may be substituted by specific safeguards that consider children's age of capacity.[235] In cases where consent has been obtained, further steps should be taken to verify whether the consent indeed came from a parent, as provided for in section 8 of the GDPR.
3. Businesses and ISPs should uphold the right to erasure as provided for in the GDPR. Once a child turns 18, websites that have collected and used personal information with the explicit consent of the child or their parents should no longer be allowed to retain the information

[234] MV Cunha, 'Child Privacy in the Age of the Web 2.0 and 3.0: Challenges and opportunities for policy' (Innocenti Discussion Paper 2017-03 UNICEF 2017) 17 <www.unicef-irc.org/publications/926-child-privacy-in-the-age-of-web-20-and-30-challenges-and-opportunities-for-policy.html> accessed 21 August 2020.
[235] ibid.

gathered before the child reached the age of legal majority and should be obliged to remove the information immediately. The individual can be given an opportunity to discontinue or explicitly consent to the continued collection and use of their information and the implications thereof.

4. Businesses and ISPs should also engage in public awareness so as to educate children on online safety. Clear reporting mechanisms should be established by websites and ISPs to ensure that children and parents report cases of online abuse or any potential threats online. These mechanisms should be accompanied by adequate redress.
5. Businesses and ISPs must introduce techniques that both limit avenues for possible adult offenders to have access to abusive material and restrict children's exposure to sites, material and experiences likely to cause them harm.[236] This can be through developing effective codes of conduct, taking down illegal or harmful content immediately, and developing filters and parental control software. Businesses and ISPs should also report cases of online exploitation of children.

5.2.3 Recommendations to parents and guardians

Parents and guardians have a far greater responsibility to play in mediating and supporting their children's online practices. This includes reasonably monitoring children's online practices, educating them about online risks, how to stay safe online and encouraging them to report any abuse they experience online.

[236] UNICEF, *Child Safety Online Challenges and Strategies Technical Report* (n 231) 85-86.

BIBLIOGRAPHY

Books and Articles

Akdeniz Y, *Internet Child Pornography & the Law: National & International Responses* (Ashgate 2008)

Bulger M and others, 'Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online' (2017) 19 Sarah and George Journals 7

Byrne J and Burton P, 'Children as Internet users: how can evidence better inform policy debate?' (2017) 2 Journal of Cyber Policy 40

Dooley J, Pyzalski J and Cross D, 'Cyberbullying versus face-to-face bullying: A theoretical and conceptual review' (2009) 4 Journal of Psychology 106

Feltoe G, 'Strengthening our law on child sexual abuse' (2017) 1 Zimbabwe Electronic Law Journal 6

Hoofnagle CJ, Van Der Sloot B and Borgesius FZ, 'The European Union General Data Protection Regulation: what it is and what it means' (2016) 28(1) Information & Communications Technology Law 65

Jaishankar J, *Cyber criminology: Exploring Internet Crimes and Criminal Behaviour* (CRC Press 2011)

Jasmontaite L and Hert D, 'The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet' (2015) 5 International Data Privacy 7

Kleijssen J and Perri P, 'Cybercrime, Evidence and Territoriality: Issues and Options' in Kuijer W and Werner W (eds), *Netherlands Yearbook of International Law* (TMC Springer: Asser Press 2016)

Kshreti N, 'Cybercrime and Cyber Security in Africa' (2019) 22 Journal of Global Information Technology Management 78

Livingstone S and O'Neill B, 'Children's rights online: challenges, dilemmas and emerging directions' in van der Hof S, van den Berg B and Bart S (eds), *Minding Minors Wandering the Web: Regulating Online Child Safety Information technology and law series* (Springer Asser Press 2014)

Makulilo AB, 'Privacy and data protection in Africa: A state of the art' (2012) 2(3) International Data Privacy Law 163

Raskauskas J and Stoltz AD, 'Involvement in Traditional and Electronic Bullying among Adolescents Developmental Psychology' (2007) 43 American Psychological Association 564-575
Saki O, *Internet governance in Zimbabwe: An analysis of legislation that has an impact on the use of the internet* (MISA Zimbabwe 2016)
Schwartz P and Peifer KN, 'Transatlantic data privacy law' (2017) 106(1) The George Town Law Journal 123
Staksrud E, *Children in Online World Risk, Regulation, Rights* (Ashgate 2013)
Terblanche SS and Mollema N, 'Child Pornography in South Africa' (2011) 24 South African Journal of Criminal Justice 286
UNICEF, *Implementation handbook for the Convention on the Rights of the Child* (UNICEF: Atar Roto Presse 2007)

Official documents

African Union Commission (AUC) and Symantec 'Cyber Crime and Cybersecurity Trends in Africa' (AUC and Symantec 2016) 53.
Burton P, Leoschut L and Phyfer J, 'South African Kids Online: A glimpse into children's internet use and online activities' (The Centre for Justice and Crime Prevention 2016) <www.cjcp.org.za/uploads/2/7/8/4/27845461/south_africa_kids_online_full_report.pdf> accessed 24 May 2020
Children's Commissioner of England, 'Growing Up Digital: A report of the Growing Up Digital Taskforce' (Children's Commissioner of England 2017) <www.childrenscommissioner.gov.uk/report/growing-up-digital/> accessed 24 May 2020
Cunha MV, 'Child Privacy in the Age of the Web 2.0 and 3.0: Challenges and opportunities for policy' (Innocenti Discussion Paper 2017-03 UNICEF 2017) <www.unicef-irc.org/publications/926-child-privacy-in-the-age-of-web-20-and-30-challenges-and-opportunities-for-policy.html> accessed 21 August 2020
ECPAT International and Religions for Peace, 'Protecting Children from Online Sexual Exploitation: A guide to action for religious leaders and communities' (ECPAT International and Religions for Peace 2016) <www.unicef.org/media/66776/file/Guide-for-Religious-Leaders-and-Communities-ENG.pdf> accessed 21 August 2020
Ghana Country Report, 'Risks and opportunities related to child online practices' (2017) 17 <www.unicef.org/ghana/media/1791/file/Risks%20and%20Opportunities%20-%20Child%20Online%20Protection.pdf> accessed 16 August 2020
Global Partners Digital, 'UN Committee on the Rights of the Child: Concept note for a General Comment on children's rights in relation to the digital environment' (Global Partners Digital Submission 2019) <www.gp-digital.org/wp-content/uploads/2019/05/CRC-Children%E2%80%99s-Rights-in-Relation-to-the-Digital-Environment-GPD-Submission-GPD-Template-1.pdf> accessed 13 September 2020

Information Commissioner's Office, 'Children and the GDPR' (*ICO*, 2018) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/> accessed 12 October 2020

International Centre for Missing and Exploited Children, 'Child Pornography: Model Legislation & Global Review' (International Centre for Missing and Exploited Children 2012) <www.icmec.org/wp-content/uploads/2015/10/7th-Edition-EN.pdf> accessed 12 October 2020

Krivokapić D and Adamović J, 'Impact of general data protection regulation on children's rights in digital environment' (2016) 205-206 <www.researchgate.net/publication/312355507_Impact_of_general_data_protection_regulation_on_children's_rights_in_digital_environment> accessed 13 September 2020

Livingstone S, Carr J and Byrne J, 'One in Three: Internet Governance and Children's Rights' (UNICEF Innocenti Discussion Paper 2016-01 UNICEF 2016) <www.unicef-irc.org/publications/pdf/idp_2016_01.pdf> accessed 24 May 2020

Microsoft, 'Digital Civility Index' (*Microsoft*, 2019) <www.microsoft.com/en-us/digital-skills/digital-civility?activetab=dci_reports%3aprimaryr5> accessed 8 September 2020

Organisation for Economic Co-operation and Development, 'The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them' (OECD 2011) <www.oecd-ilibrary.org/science-and-technology/the-protection-of-children-online_5kgcjf71pl28-en> accessed 24 May 2020

Phyfer J, Burton P and Leoschut L, 'South African Kids Online: Barriers, opportunities and risks: A glimpse into South African children's internet use and online activities' (Technical Report, Centre for Justice and Crime Prevention 2016) <http://eprints.lse.ac.uk/71267/2/GKO_Country-Report_South-Africa_CJCP_upload.pdf> accessed 13 September 2020

Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), 'Abridged Postal & Telecommunications Sector Performance Report First Quarter' (POTRAZ 2020) <www.potraz.gov.zw/wpcontent/uploads/2020/06/Sector_Performance_1stQ2020.pdf> accessed 8 September 2020

—, 'Child Online Protection Guidelines for Children' (POTRAZ 2015) <www.potraz.gov.zw/wp-content/uploads/2015/05/POTRAZ_COP.pdf> accessed 13 September 2020

UNCRC 'Report on the eleventh session' (22 March 1996) UN Doc CRC/C/50

UNICEF, 'Child Safety Online Global Challenges and Strategies Technical Report' (UNICEF 2012) <www.unicef-irc.org/publications/652-child-safety-online-global-challenges-and-strategies-technical-report.html> accessed 13 September 2020

—, 'Children's online privacy and freedom of expression' (Industry toolkit, UNICEF 2018)<www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf> accessed 24 May 2020

—, 'Children's Rights and Business in a Digital World: Privacy, protection of personal information and reputation' (Discussion Paper Series, UNICEF 2017) <www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf> accessed 12 September 2020

UNICEF, 'Children's Rights and the Internet: From Guidelines to Practice' (UNICEF 2016) <www.unicef.org/csr/files/Childrens_Rights_and_the_Internet_Guidelines_to_Practice_Guardian_Sustainble_Business_English.pdf> accessed 21 October 2020
— 'The State of the World's Children: Children in a Digital World' (UNICEF 2017) <www.unicef.org/reports/state-worlds-children-2017> accessed 8 September 2020., 'Children's online privacy and freedom of expression' (Industry toolkit, UNICEF 2018)<www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf> accessed 24 May 2020
—, 'Children's Rights and Business in a Digital World: Privacy, protection of personal information and reputation' (Discussion Paper Series, UNICEF 2017) <www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf> accessed 12 September 2020
—, 'Children's Rights and the Internet: From Guidelines to Practice' (UNICEF 2016) <www.unicef.org/csr/files/Childrens_Rights_and_the_Internet_Guidelines_to_Practice_Guardian_Sustainble_Business_English.pdf> accessed 21 October 2020
— 'The State of the World's Children: Children in a Digital World' (UNICEF 2017) <www.unicef.org/reports/state-worlds-children-2017> accessed 8 September 2020.
— and others, 'Covid-19 and its implications for protecting children online' (UNICEF 2020) <www.unicef.org/sites/default/files/2020-04/COVID-19-and-Its-Implications-for-Protecting-Children-Online.pdf> accessed 21 October 2020
—, UN Global Compact and Save the Children, 'Children's Rights and Business Principles' (2012) <www.unicef.org/documents/childrens-rights-and-business-principles> accessed 21 October 2020.

Case law

European Court of Human Rights

Hachette Filipacchi Associés v France App no 71111/01 (ECtHR, 14 June 2007)
Bogomolova v Russia App no 13812/09 (ECtHR, 20 June 2017)

USA

US v James Snyder (1999) 189 F 3d 640
US v Donald Blakley (2005) 239 F 229

South Africa

S v William Alexander Beale Case no A283/18 (3 May 2019)
S v Stevens 2007 JDR 0637 (E)
S v Kleinhas [2014] 2 SACR

Internet Sources

African Charter on the Rights and Welfare of the Child ratification list <https://au.int/sites/default/files/treaties/36804-sl-AFRICAN%20CHARTER%20ON%20THE%20RIGHTS%20AND%20WELFARE%20OF%20THE%20CHILD.pdf> accesed 21 October 2020

Browne R, 'Grandmother ordered to delete pictures of her grandkids on social media in EU privacy ruling' (*CNBC*, 22 May 2020) <www.cnbc.com/2020/05/22/gdpr-grandmother-ordered-to-delete-social-media-pictures-of-grandkids.html> accessed 4 October 2020

Child exploitation and Online Protection command, 'What is Online Child Sexual Abuse and Exploitation?' <www.ceop.police.uk/Safety-Centre/what-is-online-child-sexual-abuse/> accessed 16 August 2020

Childnet International, 'Online grooming and UK law' (*Childnet International*) <www.childnet.com/ufiles/online-grooming.pdf> accessed 12 October 2020

ChildSafeNet, 'Cyber Grooming' (*ChildSafeNet*) <www.childsafenet.org/new-page-15> accessed 22 August 2020

Council of Europe Commissioner for Human Rights, 'Protecting children's rights in the digital age: An ever-growing challenge' (*Council of Europe*, 2014) <www.coe.int/en/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen-1> accessed 24 May 2020

Elgersma C, 'Parenting, Media, and Everything in Between: 18 Social Media Apps and Sites Kids Are Using Right Now' (*Common Sense Media*, 6 June 2019) <www.commonsensemedia.org/blog/16-apps-and-websites-kids-are-heading-to-after-facebook> accessed 14 September 2020

EU Child Protection Convention Chart of signatures and ratifications of treaty 201 <www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=201 > accessed 21 October 2020

EU Convention on Cybercrime Chart of signatures and ratifications of treaty 185 <www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185> accessed 21 October 2020

EUR-Lex Access to European Union Law, 'The general data protection regulation applies in all Member States from 25 May 2018' (*EUR-Lex*, 24 May 2018) <https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html#:~:text=Share-,The%20general%20data%20protection%20regulation%20applies%20in%20all%20Member%20States,Directive%2095%2F46%2FEC> accessed 12 October 2020

Federal Communications Commission, 'Children's Internet Protection Act' (*Federal Communications Commission*, 30 December 2019) <www.fcc.gov/consumers/guides/childrens-internet-protection-act> accessed 11 October 2020

Independent Communications Authority South Africa, 'State of the ICT Sector Report in South Africa' (Independent Communications Authority South Africa 2020) <www.icasa.org.za/legislation-and-regulations/state-of-the-ict-sector-in-south-africa-2020-report> accessed 12 September 2020

Jantjies M, 'Kids can keep learning even during a lockdown. Here is how' (*The Conversation*, 26 March 2020) <https://theconversation.com/kids-can-keep-learning-even-during-a-lockdown-heres-how-134434> accessed 24 May 2020

Lexico Oxford English and Spanish Dictionary, 'Internet' (*Lexico*) <www.lexico.com/definition/internet> accessed 16 August 2020

Malabo Convention ratification list as at 18 June 2020 < https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf > accessed 21 October 2020.

Moody G, 'French Parents Face Fines, Lawsuits and Prison for Posting Pictures of Their Own Children Online' (*Tech Dirt*, 7 March 2016) <www.techdirt.com/articles/20160302/07480733781/french-parents-face-fines-lawsuits-prison-posting-pictures-their-own-children-online.shtml> accessed 4 October 2020

NI Direct, 'Social media, online gaming and keeping children safe online' (*NI Direct*) <www.nidirect.gov.uk/articles/social-media-online-gaming-and-keeping-children-safe-online> accessed 14 September 2020

NSPCC, 'Grooming' (*NSPCC*) <www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/> accessed 21 August 2020

— 'Online abuse' (*NSPCC*) <www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/online-abuse/> accessed 16 August 2020

Polity, 'Delivering education online: coronavirus underscores what's missing in Africa' (*Polity*, 20 April 2020) <www.polity.org.za/article/delivering-education-online-coronavirus-underscores-whats-missing-in-africa-2020-04-20> accessed 8 September 2020

Save the Children, 'Children's online safety a priority in Zimbabwe' (*Save the Children Zimbabwe*, 1 November 2018) <https://zimbabwe.savethechildren.net/news/childrens-online-safety-priority-zimbabwe> accessed 21 August 2020

The United States Department of Justice, 'Citizens' Guide to US Federal Law on Child Pornography' (*The US Department of Justice*, 28 May 2020) <www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography> accessed 12 October 2020

United Nations Human Rights Office of the High Commissioner Status of ratification Interactive Dashboard<https://indicators.ohchr.org/ > accessed 21 October 2020

United States Code (1994 until present) <www.govinfo.gov/help/uscode#:~:text=The%20United%20States%20Code%2C%20is,was%20first%20published%20in%201926> accessed 12 October 2020

International and regional instruments

African Charter on the Rights and Welfare of the Child (adopted 1 July 1990, entered into force 29 November 1999) CAB/LEG/24.9/49 (1990) (African Children's Charter)

African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014)

Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Child Protection Convention) (ECHR)

Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC)

Council of Europe Convention on Cybercrime 2001 (Budapest Convention) (ECHR)

International Telecommunication Union Resolution 179 (REV.BUSAN, 2014) (ITU)

Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (adopted 25 May 2000, entered into force 18 January 2002) A/RES/54/263) (OPSC)

SADC Model Law on Data Protection (2013)

UN Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework as annexed to the Report of the Special Representative of the United Nations Secretary-General on the issue of human rights and transnational corporations and other business enterprises (21 March 2011) A/HRC/17/31, United Nations, endorsed by the United Nations Human Rights Council in A/HRC/RES/17/4

UNCRC, 'General Comment 13 on the right of the child to freedom from all forms of violence' (18 April 2011) UN Doc CRC/C/GC/13

—, Draft General Comment 25 on children's rights in relation to the digital environment (2020)

Legislation

South Africa

Children's Act 38 of 2005

Constitution of South Africa 108 of 1996

Consumer Protection Act 68 0f 2008

Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007

Cybercrimes Bill

Electronic Communications Transaction Act 25 of 2002

Protection from Harassment Act 17 of 2011

Protection of Personal Information Act 4 of 2013

Regulation of Interception of Communications and Provision of Communication-related information Act 70 0f 2002

South African Films and Publications Amendment Act 11 of 2019

ZIMBABWE

Censorship and Entertainment Controls Act 22 of 2001
Children's Act 23 of 2001
Constitution of Zimbabwe Act 20 of 2013
Consumer Protection Act 5 of 2019
Criminal Law (Codification and Reform) Act 23 of 2004
Cyber-Security and Data Protection Bill
Freedom of Information Act 1 of 2020
Interception of Communications Act 6 of 2007
Public Health (Covid-19 Prevention, Containment & Treatment) (National Lockdown) Order SI 83 of 2020
Sexual Offences Act 8 of 2001

EUROPEAN UNION

General Data Protection Regulation (GDPR)

USA

Children Internet Protection Act 2000
United States Code 1994

NEWSPAPERS

MISA Zimbabwe, 'Online abuse and the law' *Zimbabwe Mail* (Harare, 6 November 2019)

Global Campus of Human Rights

Monastery of San Nicolò
Riviera San Nicolò, 26
I-30126 Venice Lido (Italy)

www.gchumanrights.org

Global Campus of Human Rights

The Global Campus of Human Rights is a unique network of more than one hundred participating universities around the world, seeking to advance human rights and democracy through regional and global cooperation for education and research. This global network is promoted through seven Regional Programmes which are based in Venice for Europe, in Sarajevo/Bologna for South East Europe, in Yerevan for the Caucasus, in Pretoria for Africa, in Bangkok for Asia-Pacific, in Buenos Aires for Latin America and the Caribbean, and in Beirut for the Arab World.

The Global Campus Awarded Theses

Every year each regional master's programmes select the best master thesis of the previous academic year that is published online as part of the GC publications. The selected seven GC master theses cover a range of different international human rights topics and challenges.

The present thesis - ***Protection of Children's Rights to Privacy and Freedom from Online Exploitation and Abuse in Southern Africa. A Case Study of South Africa*** and Zimbabwe written by **Opal Masocha Sibanda** and supervised by Zahara Nampewo, Makerere University (Uganda) and Marystella Simiyu, University of Pretoria - was submitted in partial fulfillment of the requirements for the Master's Programme in Human Rights and Democratisation in Africa (HRDA), coordinated by Centre for Human Rights, University of Pretoria.

This document has been produced with the financial assistance of the European Union and as part of the Global Campus of Human Rights. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or of Global Campus of Human Rights