ENSURING CHILD ONLINE SAFETY IN THE DIGITAL AGE: A CASE STUDY OF MOSHATE VILLAGE, LIMPOPO

Ms. Tsholofelo Mokone[1], and Adv. Lerato Seema[2].

[1] Tsholofelo Mokone, Internet Governance - Compliance, and Regulations, ZA Domain Name Authority, Johannesburg, South Africa (*Contributor*)

[2] Lerato Seema, Executive Manager – Compliance and Regulations, ZA Domain Name Authority, Johannesburg, South Africa (*Contributor*)

ABSTRACT

South Africa annually commemorated National Child Protection Week, emphasising the protection of children's rights as enshrined in the Constitution and the Children's Act. Although these legal frameworks aim to safeguard children, violations of these rights persist, particularly as the increased use of the internet exposes children to risks such as cyberbullying, online exploitation, and child trafficking. Studies by UNICEF South Africa, and the Department of Social Development have highlighted the growing prevalence of online abuse, with children frequently engaging in risky online behaviour. As part of its role during Child Protection Week, the ZA Domain Name Authority (ZADNA) led workshops in Limpopo to raise awareness about online safety, focusing on equipping parents and law enforcement with strategies to mitigate these risks.

This case study examines ZADNA's contributions and emphasises the importance of balancing children's online safety with the freedom to explore the internet's educational benefits. It also discusses the awareness of parents, guardians, and law enforcement in managing online safety, highlighting the challenges they face due to generational gaps in digital literacy. Finally, the study explores the risks associated with Domain Name System (DNS) abuse and its impact on children. It offers recommendations for improving child online safety through collaborative efforts involving schools, parents, and government stakeholders. The case demonstrates the need for comprehensive education and more robust law enforcement mechanisms to protect children in the digital age.

Keywords: *Child Protection, Children's Rights, Online Safety, Cyberbullying, Online Exploitation, ZA Domain Name Authority (ZADNA), Digital Literacy, Domain Name Systems Abuse, Internet Safety, Cyber Risks, Child Online Abuse, Parental Involvement, Collaborative Efforts*

1. INTRODUCTION

The rapid advancement of digital technologies has transformed children's lives, bringing unprecedented opportunities for learning, entertainment, and communication[1]. However, with these benefits come significant risks, mainly related to children's safety online. National Child Protection Week in South Africa, commemorated annually, aims to raise awareness about the protection of children's rights[2], as articulated in the Constitution of the Republic of South Africa[3] and the Children's Act[4].

This case study explores the vulnerabilities children face online, focusing on South Africa's efforts to address these challenges through the National Child Protection Week,

[1] Haleem, A., Javaid. M., Qadri, M. A., and Suman, R. 2021. Understanding the role of digital technologies in education: A review. Available at: https://doi.org/10.1016/j.susoc.2022.05.004 [Accessed: 19 September 2024]

[2] University of Cape Town. 2020. Child Protection Week. Available at: https://hr.uct.ac.za/sites/default/files/content_migration/hr_uct_ac_za/386/files/PSG_Child_protection_week.pdf [Accessed 19 September 2024].

[3] Republic of South Africa. (1996). The Constitution of the Republic of South Africa. Government Gazette, No. 17678. Available at: https://www.gov.za/documents/constitution-republic-south-africa-1996

[4] Republic of South Africa. (2005). Children's Act (Act No. 38 of 2005). Government Gazette, No. 28944. Available at: https://www.gov.za/documents/childrens-act

particularly the role of the ZA Domain Name Authority (ZADNA).

2. ZADNA'S ROLE IN THE NATIONAL CHILD PROTECTION WEEK

As a statutory entity established to manage and regulate the .za namespace, ZADNA through its Internet Governance function participated in National Child Protection Week aimed at strengthening the protection of children online. The event was attended by parents and law enforcement officials, who discussed the risks posed by the internet, including DNS abuse. The primary goal was to provide parents with strategies for monitoring their children's online activities and to equip law enforcement officials with the knowledge to address Domain Name Systems (DNS) crimes affecting children.

3. CHILD ONLINE SAFETY IN SOUTH AFRICA

Child online safety broadly refers to protecting children, learners, and students while using the internet, allowing them to explore its benefits without facing harm[5]. The aim is to create a secure online environment through awareness and education, rather than imposing overbearing restrictions, such as excessive monitoring or forbidding access to social media. According to the eSafety Commission (2022), online safety should involve finding a balance—ensuring that children are safe online while also encouraging them to explore the internet's resources responsibly[6].

The internet presents several risks to children, including exposure to inappropriate content, solicitation by sexual predators, online bullying, inappropriate disclosure of personal information, and data theft. Cyberbullying is one of the most visible risks. This refers to the use of digital technologies, such as social media, websites, text messages, and online platforms, to deliberately harass, threaten, embarrass, or target another person[7]. According to Hinduja and Patchin[8] (2018), it involves repeated aggressive behaviour intended to harm or intimidate someone, often through spreading rumors, personal attacks, or inappropriate content. Cyberbullying can occur in various forms, including sending harmful messages, sharing sensitive or private information without consent, or creating fake profiles to impersonate or ridicule the victim. It can happen anytime, making it particularly distressing for the victim.

Cyberbullying is a growing concern in South Africa, with the prevalence of online harassment and intimidation on the rise. According to the South African Depression and Anxiety Group (SADAG), a survey conducted by the Mandela Metropolitan University study found that 37% of students reported experiencing cyberbullying[9]. This alarming trend is further exacerbated by the fact that many young people are unaware of how to handle online harassment, with only 37% of respondents in a survey conducted by the Centre for Justice and Crime Prevention (CJCP) indicating that they knew how to respond to cyberbullying[10]. The consequences of cyberbullying can be severe, with victims experiencing emotional distress, anxiety, depression, and even suicide. A notable case from Limpopo Province involved the suicide of a teenager who had been cyberbullied, shedding light on the devastating impact this behaviour can have[11].

However, cyberbullying is just one aspect of a broader set of online dangers that threaten the safety and well-being of children in South Africa. Another alarming issue is the circulation of Child Sexual Abuse Material (CSAM) on social media platforms, which constitutes a grave violation of children's rights. CSAM often involves the exploitation and victimisation of minors, with images and videos disseminated without the consent of the victims, further traumatising them

[5] Broadband Commission. 2019. Child Online Safety: Minimising the risk of abuse, violence, and exploitation online. Available at: https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf [Accessed:19 September 2024].

[6] eSafety Commission. 2022. Keeping children safe online advice for parents and carers. Available at: https://www.esafety.gov.au/sites/default/files/2022-03/Keeping%20children%20safe%20online%20-%20advice%20for%20parents%20and%20carers%20%28English%29.pdf [Accessed: 19 September 2024]

[7] Reddy, S. Providing a legal definition for cyberbullying in South Africa. Available at: https://scielo.org.za/pdf/obiter/v44n4/03.pdf [Accessed: 20 September 2024].

[8] Hinduja S., Patchin J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. Deviant Behavior, 29(2), 129–156. https://doi.org/10.1080/01639620701457816 [Accessed 21 September 2024].

[9] POPOVAC, M. 2012. Cyberbullying in South Africa: Impact and responses. Available at: https://www.researchgate.net/publication/259117407_Cyber_bullying_in_South_Africa_Impact_and_Responses [Accessed: 21 September 2023]

[10] IBID. (2012)

[11] Sonjica, N. 2021. Limpopo pupil allegedly commits suicide after being bullied at school. TimesLive. Accessed at: https://www.timeslive.co.za/news/south-africa/2021-04-13-limpopo-pupil-allegedly-commits-suicide-after-being-bullied-at-school/ [Accessed on the 22 September 2024].

and violating their dignity[12]. Though CSAM is illegal in South Africa[13], the ease of sharing content on social media accelerates the spread of such material, making it challenging for authorities to monitor and control. This issue not only endangers the immediate safety of the victims but also perpetuates a cycle of abuse, as perpetrators feel emboldened by the anonymity that the internet provides.

Addressing these issues requires collaboration between government and stakeholders in educating youth on internet safety practices, such as reporting cyberbullying and avoiding interactions with unknown individuals online. By fostering a culture of digital responsibility, children can be empowered to navigate the internet safely while benefiting from its vast educational and social opportunities. With the growing digital presence of young people, parents and guardians must actively engage in their children's online activities.

4. CASE STUDY: PARENTS AND GUARDIANS' KNOWLEDGE AND PRACTICES OF ONLINE SAFETY

During a 2021 Child Online Safety workshop held in Moshate Village, Mokopane, a critical issue emerged: many parents, particularly those from lower socio-economic backgrounds, lacked sufficient digital literacy to manage their children's online safety effectively. This gap in digital knowledge leaves children more exposed to online risks, especially as their time spent on the internet has increased dramatically since the COVID-19 pandemic.

For parents in Moshate Village, the unfamiliarity with the internet and social media platforms has created a significant challenge in supervising their children's online activities. While young people, often referred to as "digital natives," have grown up with the internet as an integral part of their lives, their parents struggle to navigate these spaces. This has led to a growing concern among parents about their children's online behaviour, safety, and exposure to potentially harmful content.

One of the workshop's key takeaways was the limited awareness among parents of the tools and strategies available for online safety. Parents shared that they often rely on offline strategies to control their children's internet usage. These strategies include restricting access to the internet altogether or resorting to informal, unstructured education about the dangers of the online world. For instance, some parents set strict rules about when their children can access the internet, but these methods are not always effective, especially as children grow older and more autonomous in their internet use.

The need for more formal and structured cybersafety education was a recurring theme in the workshop discussions. Parents strongly desire schools to take a more active role in teaching children about online safety, particularly the risks associated with social media, cyberbullying, and inappropriate content. They felt that schools, as institutions of learning, are better positioned to deliver comprehensive education on these topics and can complement the efforts made by parents at home. This dual approach—combining family values with formal education—was seen as a critical solution to improving online safety for children.

Moreover, parents in Moshate Village acknowledged their lack of understanding of online security settings and parental control tools that could help them manage their children's Internet usage more effectively. Many parents admitted that they did not know how to use features like privacy settings, content filters, or time restrictions, which could help protect their children from exposure to inappropriate content. This lack of knowledge exacerbates their difficulties in keeping their children safe online.

The parents highlighted the urgent need for education and support in this area. They called for workshops or training programs that would teach them how to use online safety tools and understand the digital spaces their children inhabit. Furthermore, parents emphasised the importance of involving schools in creating a holistic approach to cyber safety that incorporates formal education, family values, and practical skills for managing online risks.

5. THE IMPACT OF DNS ABUSE ON CHILD ONLINE SAFETY

Limited knowledge of Domain Name Systems (DNS) abuse among law enforcement officials is another growing concern, and poses significant risks to children, particularly as harmful content is increasingly hosted on deceptive domain names. DNS abuse refers to the exploitation of domain names to facilitate illegal or harmful activities online, including hosting malicious content, phishing schemes, and distributing child

[12] Chauviré-Geib K, Fegert JM. Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. Trauma Violence Abuse. 2024 Apr;25(2):1335-1348.

[13] Mathebula, Z. 2016. An overview on the law on child pornography in South Africa. Available at: https://www.ppmattorneys.co.za/an-overview-on-the-law-on-child-pornography-in-south-africa/ [Accessed 23 September 2024]

CSAM[14]. DNS abuse is a challenge both in South Africa and globally, particularly in its implications for child safety.

One of the most concerning forms of DNS abuse involves websites that distribute CSAM. These sites often use misleading domain names to attract children or individuals seeking explicit content, leading them to inadvertently encounter harmful material[15].

In South Africa, posting CSAM is illegal[16] . According to the Films and Publications Act[17] of 1996 and the Criminal Law (Sexual Offences and Related Matters) Amendment Act[18] of 2007, it is a criminal offense to unlawfully and intentionally expose or display, or cause the exposure or display, of any material involving child pornography or content of a sexual nature featuring a child. This applies to any image, publication, or depiction, regardless of the child's consent, and includes material that may be disturbing, harmful, or inappropriate for children.

In addition to CSAM, DNS abuse is frequently used to impersonate reputable brands or institutions through phishing. Scammers register domain names that closely resemble legitimate ones, tricking users into providing personal information. This is particularly alarming for children, who may be less cautious online and thus more susceptible to identity theft and financial exploitation[19].

Another form of DNS abuse involves the distribution of malicious software. Some domains are created specifically to distribute malware disguised as legitimate applications or content, which children might unknowingly download[20]. This can lead to compromised devices and further exposure to online risks, including cyberbullying and exploitation. Additionally, DNS abuse can manifest in the creation of malicious domains aimed at harassing individuals, including children. Perpetrators might set up fake profiles or websites to spread false information or instigate harassment, exacerbating the psychological effects on victims[21]

During an engagement led by the Film and Publication Board (FPB), law enforcement officials acknowledged the difficulties in consistently applying the law against offenders engaged in DNS abuse. One significant challenge is the underreporting of abuses, often due to fear of repercussions or a lack of awareness among victims, particularly children. When the perpetrator is a familiar figure, such as a family member or acquaintance, the likelihood of reporting decreases significantly.

To combat the risks associated with DNS abuse, several measures are essential. First, increasing awareness and education among parents, guardians, and children about the dangers of DNS abuse is crucial. Workshops and community programs can inform them about recognising and reporting suspicious online activities. Second, collaboration among stakeholders—including government agencies, law enforcement, schools, and organisations like ZADNA and FPB—should be enhanced to create comprehensive strategies that protect children online. This includes sharing resources and information about emerging threats.

Furthermore, law enforcement agencies should receive specialised training to address the unique challenges posed by DNS abuse, including understanding the technology behind domain registration and monitoring suspicious activities. Establishing user-friendly and confidential reporting channels for victims of online abuse can encourage more individuals to come forward without fear of stigma or repercussions.

As the digital landscape continues to evolve, the risks associated with DNS abuse will likely grow. Fostering a collaborative approach among stakeholders and increasing awareness can better protect children from the harmful effects of DNS abuse, ensuring a safer online environment for future generations.

6. RECOMMENDATIONS

The increased internet use among children offers numerous benefits, from educational opportunities to social connections. However, these benefits are accompanied by significant risks. To address these challenges, adopting a multi-faceted approach involving parents, schools, government entities, and

[14] Bayer, J., Yevheniya, N., Hureau, O., Fernandez, S., and Maciej, K. (2022). Study on Domain Name System (DNS) Abuse: Technical Report.
[15] We Protect Global Alliance. 2023. Global Threats Assessment. Available at: https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf [Accessed 23 September 2024]
[16] ABID (2019)
[17] Films and Publications Act 1996, No. 65 of 1996, Government Gazette, Republic of South Africa.
[18] Criminal Law (Sexual Offences and Related Matters) Amendment Act 2007, No. 32 of 2007, Government Gazette, Republic of South Africa.
[19] Krone, T. and Smith, R. G. 2018. Criminal misuse of the Domain Name System. Available at: https://www.aic.gov.au/sites/default/files/2020-05/research_report_03.pdf [Accessed 23 September 2024].
[20] Mallick, Md & Nath, Rishab. 2024. Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments.
[21] ABID. (2024)

organisations like ZADNA is essential. The following recommendations are made:

Digital Literacy Education: Schools should implement formal cyber safety programs to educate young people about online risks and how to protect themselves. These programs should also extend to parents, helping bridge the generational gap in digital literacy.

Parental Support: Parents need guidance on monitoring their children's online activities without restricting their freedom. Community workshops and online safety resources should be provided to help parents understand the digital landscape.

Law Enforcement Training: Law enforcement officials require better training to handle DNS abuse and other forms of online exploitation. Additionally, efforts should be made to encourage reporting by creating safe and supportive environments for children to disclose online abuse.

Collaborative Efforts: Stakeholders such as ZADNA, FPB, and other child protection organisations must collaborate on campaigns that raise awareness of child online safety. These campaigns should include practical tools and guidelines for young people, parents, and educators.

8. CONCLUSION

The internet presents both opportunities and risks for children, and ensuring their safety online is a shared responsibility among parents, schools, government agencies, and internet authorities like ZADNA. The annual National Child Protection Week highlighted the vulnerabilities children face online, from cyberbullying to exposure to inappropriate content. The case study demonstrates that while children may be aware of online risks, they often lack the knowledge or resources to protect themselves. Similarly, parents and law enforcement face challenges in adapting to the rapidly evolving digital landscape.

By enhancing digital literacy, supporting parents, and strengthening law enforcement, South Africa can create a safer online environment for its children, enabling them to reap the benefits of the internet while minimizing the risks. The work of ZADNA and other stakeholders in this space remains critical in the ongoing effort to protect children's rights in the digital age.