

Input Submission to the Special Rapporteur on the Sale and Sexual Exploitation of Children – to inform the Special Rapporteur’s forthcoming report to the 79th session of the UN General Assembly in October 2024.

Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment

14 May 2024

About:

Kabukabu Laura Lisita | Ph.D. Graduand for the Degree Doctor of Laws with International Aspects of Law (Child Rights – Worst Forms of Child labour and Education Rights), North-West University, South Africa. | Researcher/Trainer/Independent Child Rights Consultant | www.linkedin.com/in/laura-kabukabu-lisita

Career summary | Ph.D. Graduand poised to earn a Doctor of Laws Degree with a focus on International Aspects of Law (Child Rights). Proven expertise as a Researcher, Trainer, Guest Lecturer, and Independent Child Rights Consultant. Adept at merging legal scholarship with practical applications, driving innovation in legal practice with diligence, leadership and strategic vision. Passionate about shaping the future of law as regards the intersection of Child Rights and Technology through insightful research, impactful training initiatives, and strategic consulting.

The opportunity to share insights with the Special Rapporteur on the Sale and Sexual Exploitation of Children, in response to existing and emerging sexually exploitative practices against children in the digital environment is highly welcome. It is indeed timeous and relevant. With a focus on Artificial Intelligence (AI) technology especially, I present my input on question 4 as outlined in the Call for Input:

4. What are the challenges that exist in the use of these digital technologies, products or services, that inhibit the work of law enforcement across jurisdictions in their work to investigate, detect, remove child sexual abuse materials online and prosecute these crimes?

1 Introduction

Combatting child sexual abuse materials (CSAM) in the digital realm intersects with the risks posed by emerging technologies to children’s safety. Such technological advancements include the Metaverse and Virtual Reality or Extended Reality more broadly, as well as AI. Online CSAM offences encompass various technologically facilitated activities like production, preparation, viewing, sharing, and possession of representations that depict children in sexually exploitative ways.¹ AI systems are particularly highlighted herein given that AI is designed to emulate intelligent behaviours such as reasoning, learning, perception, prediction, planning, and control.² AI’s utilisation in this way influences decision-making, communication, and

¹ Maxwell 2023 *The International Journal of Children’s Rights* 62.

² UNESCO *Recommendation on the Ethics of Artificial Intelligence* 10.

information processing to a higher degree than other technological advancements. AI in this light is deployed and embedded in already existing technologies that underlie human-computer interface such as email, text messages, instant messaging and social media platforms.³

In the context of the work of law enforcement in tackling CSAM, AI possesses the capacity to monitor and summarize large amounts of data, thereby proving invaluable in aiding law enforcements detection efforts that rely on data analysis.⁴ In this light, AI technology holds promise for law enforcement in international and national law contexts for aiding CSAM detection and removal. At the same time, however, AI's inherent limitations and associated harms include exacerbating the proliferation of CSAM in the digital environment, whereby offenders can use AI to produce and distribute CSAM in larger quantities, and ultimately impede detection efforts of this abuse. As an illustration, the Stanford Internet Observatory uncovered more than 3,200 images suspected of being CSAM within the AI database called LAION, which is an index of online images and captions used to train leading AI image recognition systems.⁵ Offenders can also readily communicate and exchange substantial amounts of CSAM through AI embedded peer-to-peer file sharing and encrypted channels, all while maintaining anonymity in the dark web setting.⁶ In view of this background, the input highlights key challenges posed by digital technologies and particularly by AI systems, for law enforcement tackling online CSAM. It gives recommendation for action thereto.

2 Identification of 4 key challenges in the use of digital technologies in the context of combating CSAM

Algorithmic biases inherent in AI models can impede efforts to detect CSAM. Where AI is deployed by law enforcement in the detection of CSAM, biased data inherent in AI models can impede their work. Such data for instance can be culturally insensitive, can exacerbate harm caused by CSAM, or can exclude certain groups of children from being identified as being at risk. Bias can be deduced through "skewed data sets, faulty algorithmic design, and negligence in the development process".⁷ The given examples are referred to as avoidable bias, and therefore can be rectified.⁸ By implication, a distinction in bias is made to that which is unavoidable. Unavoidable bias cannot easily be rectified and includes for example content that is difficult to eliminate due to factors such as "conflicting fairness principles, the complexity of the data, or the limitations of current AI technologies".⁹

³ Minnaar 2024 *Child Abuse Research in South Africa* 1.

⁴ *Comment of the Center for AI & Digital Policy (CAIDP) to the National Institute of Standards and Technology. In response to Request for Information (RFI) Related to NIST's Assignments under section 4.1, 4.5 and 11 of the Executive Order Concerning Artificial Intelligence (Sections 4.1, 4.5, and 11)* 6.

⁵ *Ibid.* 11.

⁶ Maxwell 2023 *The International Journal of Children's Rights* 63.

⁷ Tshilidzi Marwala, *United Nations University Technology Brief No.4, February 2024. Avoidable and Unavoidable Algorithmic Bias* 2.

⁸ *Ibid.* 2.

⁹ *Ibid.* 2.

For law enforcement authorities tackling CSAM, it is opined that navigating the challenges associated with avoidable and thus rectifiable bias should be of immediate priority. Questions to be considered include for instance whether data systems detecting CSAM, by virtue of their algorithmic design, are non-discriminatory. That is to say that deployed AI algorithms in the work of law enforcement tackling CSAM should be representative and inclusive of a diverse child population.¹⁰

Concerns in AIs failure to erase CSAM, and privacy concerns in the protection of children's data. AI's ability to store vast quantities of data implies that CSAM could remain accessible long after its initial posting, thereby perpetuating risks for victims and complicating law enforcements efforts to eliminate such material. Even if content is deleted from one platform, it might still be present on other platforms or duplicated and circulated across the Internet. AI's capacity to retain and preserve data thus presents a distinct challenge to law enforcement by potentially enabling the continuous online circulation of CSAM, consequently embedding child victimization in the digital landscape over the long term.¹¹

Interlinked to the above problem is the issue of safeguarding children's data privacy. Privacy stands as a right crucial for upholding the dignity and autonomy of children. Children's privacy must therefore be given due recognition in the context of law enforcement's work in detecting CSAM, as regards the process of data collection, data use, data sharing and archiving. This must be done in ways that align with international legal standards.¹²

Lack of AI and digital technical expertise within law enforcement, thus impeding detection of CSAM. Sophisticated and different types of techniques are deployed in different domains of AI embedded technologies. For instance, CSAM offenders may use techniques such as encryption and anonymized networks to evade access to and interception of their communications, as such making the tracking, finding and reporting to law enforcement a difficult exercise.¹³ An underlying hinderance to apprehending criminal in this space is the lack of technological awareness, knowledge, and human resource capabilities of law enforcement concerning encryption, cybersecurity expertise, and digital forensics as an example.¹⁴

Legal gaps in child protection statutes, low prosecution rates of CSAM offenders, and lack of structured data to develop AI systems. Important to highlight is the fact that the work of law enforcement is itself hindered by legal gaps in child rights statutes that should address CSAM.¹⁵ For example, offences against children such as the possession and distribution of CSAM may not be explicitly defined in state legislation.

¹⁰ Minnaar 2024 *Child Abuse Research in South Africa* 11.

¹¹ Ibid 2.

¹² UNESCO *Recommendation on the Ethics of Artificial Intelligence* 21.

¹³ Johansson *Combating Online Child Sexual Abuse Material. An explorative study of Swedish Police Investigations* 9.

¹⁴ Windhoek *Statement on Artificial Intelligence in Southern Africa* (2022) 1.

¹⁵ UNICEF *Ending Online Child Sexual Exploitation and Abuse. Lessons learned and promising practices in low-and middle-income countries* 10.

This is coupled with gaps in the capacity for law enforcement in areas like digital forensics, which makes it easier for offenders to face a minimum risk of investigation and prosecution.¹⁶ In the instance of frustrations in the inability to apprehend online perpetrators of CSAM, the risk is that the crime in turn can negatively affect the priority level given to it as regards its investigation and prosecution.¹⁷

Likewise, the lack of structured data to develop AI systems and regulate them accordingly within the domestic state context can itself be a hinderance to the work of law enforcement. In this instance, limited data availability in the domestic state context would make it difficult to train effective AI models that would be unbiased within the context of detecting CSAM. That is to suggest that limited data infrastructure in AI powered solutions would indeed increase reliance on foreign and advanced data-driven AI systems, which themselves would potentially increase bias in their output in relation to the reality of CSAM's representation in the domestic context.¹⁸

3 Recommendations for action

Emphasize ethics in the development of AI technology, and support the development of digital literacy for the child. At a global level, ethical considerations should be the basis for the design and implementation of AI technologies that serve the greater good, while mitigating potential harm like bias and discrimination. The normative basis guiding the deployment of ethical AI technologies should be rooted in international and national legal frameworks,¹⁹ and in particular in child rights treaties as regards AI's application in child rights domains.

Alongside efforts to protect children from CSAM, there should be a concurrent focus on fostering digital literacy and skills among children and their caregivers whether at home or in educational institutions for instance. Children should accordingly be empowered to recognize and report instances of online CSAM, supported by accessible and child-friendly resources and environments.²⁰

Promote multifaceted collaboration in tackling CSAM, and in the governance of AI. The problem of CSAM in light of digital technologies affects both the national and international landscape considering that perpetrators and CSAM content can be located in different jurisdictions via the online space. To this end, tackling CSAM must transcend jurisdictional boundaries. Cross-jurisdictional operations such as Interpol's International Child Sexual Exploitation (ICSE) database can be given as an example in this light. This image and video

¹⁶ Witting and Angula 2020 *Comparative and International Law Journal of Southern Africa* 4-5.

¹⁷ Johansson *Combatting Online Child Sexual Abuse Material. An explorative study of Swedish Police Investigations* 22.

¹⁸ *Center for AI & Digital Policy. African Union: The Development of a Continental Strategy on AI* 4.

¹⁹ UNESCO *Recommendation on the Ethics of Artificial Intelligence* 6.

²⁰ *Resolution on the Rights of the Child in the Digital Environment A/C.3/78/L.19/Rev.1* 5.

database uses advanced software that helps victim identification specialists worldwide to analyse and compare child sexual abuse images.²¹

In essence, dialogue and collaboration should be fostered amongst a multiplicity of actors to address the problem of CSAM. In the same way, multifaceted collaborative efforts amongst key actors should be pursued in the development and governance of AI systems so as to promote ethical standards, promote data privacy safeguards, and to minimize bias and discrimination.²² Participants in dialogue and collaborative processes should include notable players like states, technology industry, civil society, academia, and importantly youth and children from diverse backgrounds.

Clear definitions of CSAM in legislative frameworks. Lack of clear definitions of online CSAM can hinder progress in its identification for law enforcement. A normative basis for defining CSAM in domestic legislative frameworks in the advent of technological advancements, must itself be embedded in already existing child rights instruments. The *United Nations Convention on the Right of the Child* (article 32 and 34),²³ together with its *Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography* (article 2),²⁴ as well as the International Labour Organization's *Worst forms of Child Labour Convention* (article 3)²⁵ are of key relevance in this regard as it pertains to international laws. These outline underlying features of CSAM in aiding the work of law enforcement, and these laws must accordingly be reconciled with domestic child protection systems.

Reconcile the age of AI and the traditional approach to child rights. Combatting CSAM in the context of emerging technologies like AI should not misguidedly be interpreted as "solving a new problem with overarching new child rights standards." While indeed the world has changed considerably since the adoption of the UNCRC over 30 years ago, the convention's approach to protecting child rights nevertheless still remains relevant in the context of tackling difficult problems like CSAM in the digital age. In this light, AI regulation in the child rights space, including in the context of data sharing and privacy laws, should be founded on the already established four General Principles of the UNCRC. These have been outlined to guide the implementation process of children's rights in all spheres. That is to suggest in essence that the principle of non-discrimination (article 2), the best interests of the child (article 3), the child's right to survival and development (article 6), and the child's right to participation (article 12), should be the basis upon which the work of law enforcement is calibrated when it comes to combatting CSAM in the digital environment.

4 Conclusion

Certainly, the advent of digital technologies has radically altered the availability of CSAM in the online space, more so with AI systems at play. As a result, law enforcement agencies are

²¹ INTERPOL 2024 <https://www.interpol.int>.

²² Tshilidzi Marwala, *United Nations University Technology Brief No.5, April 2024. Framework for the Governance of Artificial Intelligence* 1.

²³ *Convention on the Rights of the Child* (1989).

²⁴ *Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography* (2000).

²⁵ *Worst Forms of Child Labour Convention, C182* (1999).

now, more than ever, faced with multiple issues as regards their detection and investigation of CSAM crimes. Key challenges presented to law enforcement have been presented in this input, and recommendations for action given. Overall, this call for input duly presents an opportunity to contribute to the enhancement of child rights safeguards in the digital space.

ANNEX OF BIBLIOGRAPHY

International Instruments and Materials

Center for AI & Digital Policy. African Union: The Development of a Continental Strategy on AI (2024)

Comment of the Center for AI and Digital Policy (CAIDP) to the National Institute of Standards and Technology. In response to Request for Information (RFI) Related to NIST's Assignments under section 4.1, 4.5 and 11 of the Executive Order Concerning Artificial Intelligence (Sections 4.1, 4.5, and 11). (2024).

Convention on the Rights of the Child (1989).

Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (2000).

Resolution on the Rights of the Child in the Digital Environment A/C.3/78/L.19/Rev.1

Tshilidzi Marwala, United Nations University Technology Brief No.4, February 2024. Avoidable and Unavoidable Algorithmic Bias.

Tshilidzi Marwala, United Nations University Technology Brief No.5, April 2024. Framework for the Governance of Artificial Intelligence.

Windhoek Statement on Artificial Intelligence in Southern Africa (2022).

Worst Forms of Child Labour Convention, C182 (1999).

Literature

Johansson Combatting Online Child Sexual Abuse Material. An explorative study of Swedish Police Investigations

Johansson C Combatting Online Child Sexual Abuse Material. An explorative study of Swedish Police Investigations (Masters-Thesis Malmö University 2019).

Maxwell 2023 The International Journal of Children's Rights

Maxwell F "Children's Rights, The Optional Protocol and Child Sexual Abuse Material in the Digital Age" 2023 The International Journal of Children's Rights 61-88.

Minnaar 2024 Child Abuse Research in South Africa

Minnaar A "An examination of early international and national efforts to combat online child pornography and child sexual exploitation and abuse material on the Internet" 2024 Child Abuse Research in South Africa 1-26.

UNESCO Recommendation on the Ethics of Artificial Intelligence

UNESCO Recommendation on the Ethics of Artificial Intelligence (UNESCO Paris 2022).

UNICEF Ending Online Child Sexual Exploitation and Abuse. Lessons learned and promising practices in low-and middle-income countries

UNICEF *Ending Online Child Sexual Exploitation and Abuse. Lessons learned and promising practices in low-and middle-income countries* (UNICEF New York 2021).

Witting and Angula 2020 *Comparative and International Law Journal of Southern Africa*

Witting SK and Angula MP "Leveraging International Law to Strengthen the National Legal Framework on Child Sexual Abuse Material in Namibia" 2020 *Comparative and International Law Journal of Southern Africa* 1-28.

Internet Sources

INTERPOL 2024 <https://www.interpol.int>

INTERPOL 2024 *International Child Sexual Exploitation Database*
<https://www.interpol.int> accessed 13 May 2024.