**Maat for Peace’ submission to the Special Rapporteur on the sale and sexual exploitation of children, including child prostitution, child pornography, and other sexual abuse material**

Specialized reports indicate that approximately 20% of children in some member states of the United Nations have been exposed to child sexual exploitation and abuse via the Internet, which makes this phenomenon continuously increasing. In response, Maat submits this report to the concerned Special Rapporteur on the sale of children and sexual exploitation regarding current and emerging practices of sexual exploitation against children in the digital environment to assist it in preparing its report that it will submit to the seventy-ninth session of the United Nations General Assembly in October 2024. Maat would like to convey its information on this matter to the Special Rapporteur. This issue is of great importance, especially after the data showed a staggering increase of 1800 percent in the images and videos showing children being subjected to rape, torture, and digital sexual abuse in the past years, especially with the increasing reliance on the internet. In 2022, the National Center for Missing and Exploited Children in the United States received 32 million reports of online exploitation and sexual abuse of children, including 49.4 million images and 37.7 million videos from technology companies[[1]](#footnote-1). Maat hopes that the information it has will help the special rapporteur in preparing its report. Maat is guided by some of the questions in the special rapporteur's request and it’s committed to the maximum number of words specified by the rapporteur.

**First: How has technology facilitated the process of sexual exploitation and abuse of children?**

Maat documented the increasing and diverse roles of technology that facilitated the unprecedented sexual exploitation and abuse of children, as children have become among the most users of modern technological tools. The speed and increased accessibility of information and communication technology for children have led to their increased exposure to various sexual crimes. This includes the creation, dissemination, promotion, and trade of materials depicting sexual abuse of children. To shed light on the gravity of this issue, Maat would like to point out that in 2018, American technology companies referred 18.4 million cases of digital sexual assault against children to the National Center for Missing Children[[2]](#footnote-2). Since 2019, cases of sexual abuse against children worldwide have increased by 87 percent[[3]](#footnote-3). In 2023, specialized reports documented 36.2 million cases of digital sexual abuse against children online[[4]](#footnote-4), confirming that 54% of individuals aged 18 to 20 have experienced different forms of digital sexual abuse through the internet during their childhood, with 62 percent of these abuses occurring via children's personal phones, 21% through friends' mobile devices, and 17 % through laptops or computers[[5]](#footnote-5).

Digital sexual blackmail against children represents the most prominent form of digital sexual exploitation they face, Perpetrators blackmail children with their naked or sexual pictures, and in many cases, the child victim is threatened to publish his pictures publicly unless he provides additional sexual content, sexual activity, or pays money. With children's fear of the possibility of the threat going viral online, there can be negative effects on them[[6]](#footnote-6). Digital enticement also represents another prominent form of digital sexual exploitation. The numbers show the existence of 186,000 cases of digital enticement of children over the internet in the United States in 2023, a 300% increase from 2022. Digital enticement of children is a form of digital sexual exploitation of children and involves individuals communicating online with someone they believe to be a child, to commit a sexual crime[[7]](#footnote-7).

Maat notes artificial intelligence (AI) has become a key facilitator of digital sexual exploitation of children, particularly for financial gain. AI, specifically generative AI[[8]](#footnote-8), can be used to produce fake sexual images or videos using real children's images, or to create materials depicting sexual assault on children. The danger of generative artificial intelligence lies in that the resulting child abuse content hinders the identification of the real victims among the children[[9]](#footnote-9).

**Second: What are the current gaps that limit the effective implementation and application of current laws, policies, and guidelines to prevent online sexual exploitation and abuse of children?**

Maat documented some gaps that limit the effective implementation of policies aimed at preventing sexual exploitation and sexual abuse of children via the Internet. For instance, Maat noted that the United States, being one of the most capable countries in controlling digital sexual exploitation of children due to the presence of many major tech company headquarters worldwide, still has one of the most important laws aimed at eliminating digital sexual exploitation of children which is pending in the US Congress. This law is known as (The EARN IT Act) under which technology companies based in the United States are required to report suspected digital child sexual abuse materials to law enforcement agencies only if they are aware of their presence on their platforms. Additionally, it calls for the formation of a new national committee to investigate digital sexual exploitation crimes against children, especially since the current law governing digital sexual exploitation of children in the United States is considered vague, particularly regarding providing guidelines for digital platforms on what their reports should include to the National Center for the Missing and Exploited. This ambiguity in the current law has led some tech platforms to submit millions of reports annually, while others submit only a few hundred each year or do not submit any reports at all[[10]](#footnote-10). For example, Meta, the owner of Facebook, Instagram, and WhatsApp, submitted around 27 million reports to the National Center for Missing and Exploited Children regarding exploitation materials and sexual abuse of children in 2022. In contrast, Apple, which owns billions of mobile phones and iPads worldwide, reported only 234 cases[[11]](#footnote-11).

**Third: What challenges exist in the use of digital technologies or services, which hinder the work of law enforcement authorities to investigate, detect, remove and prosecute online child sexual abuse material?**

Maat has noticed some challenges that hinder the investigation of child sexual abuse materials on the internet, their discovery, removal, and recently, one of the most prominent challenges was the comprehensive encryption technology implemented in some social networking sites. On 6 December 2023, Meta announced that it would implement end-to-end encryption on private conversations and calls through Messenger. This technology included encrypting the content of messages and calls throughout the entire process, making it inaccessible to any third party during transmission unless users choose to report the information to the platform. Although this undoubtedly represents a significant technological advancement from the perspective of protecting individual data privacy, comprehensive encryption technology significantly restricts access to messages on both ends of the transmission, making it impossible for any third party to discover whether the transmitted information contains content related to child exploitation, thus unintentionally protecting criminals[[12]](#footnote-12).

Maat believes that there is another challenge facing some law enforcement agencies in investigating materials for online sexual abuse of children, especially in advanced countries such as the United States, the European Union, and Canada. It lies in the fine line between freedom of opinion and expression online and the sexual exploitation of children online. Freedom of opinion and expression is often used as an excuse to escape any charges related to the sexual exploitation of children online. For example, in Canada, there is a discussion of the Internet Harms Act proposed by the government, where the government confirms that the legislation will hold digital platforms responsible if they distribute content that includes sexual abuse of children, encourages hatred, or incites violence. According to some experts who criticized the report, the legislation will violate the constitutional rights of Canadians to freedom of expression[[13]](#footnote-13). Thus, this represents a significant challenge that hinders law enforcement authorities from investigating online sexual abuse of children.

There is a third type of challenge represented by technical challenges that are primarily related to the high cost borne by some companies to detect cases of digital sexual exploitation of children, leading to multiple deficiencies in the steps taken by some of these companies to combat these crimes against children. For example, while companies like YouTube and TikTok take steps to detect child sexual abuse during live streaming, Discord does not do so because the required tools are very costly. While TikTok uses language analysis technology to detect child sexual assault activities such as sexual extortion across all its services, Discord does not use any tools to detect this at all. Twitter uses tools to detect public content, but not for direct messages. There is also a significant variation in the languages covered by different technology companies, with Google covering at least 71 languages, TikTok 73 languages, Twitter only covering 12 languages, and Discord 29 languages. This means that many languages of the world are not covered by many companies, indicating their inability to detect many cases of digital sexual exploitation against children in a range of countries. Maat received certificates from Ethiopia indicating that during the conflict between the federal government and the Tigray Liberation Front. The incidents of violating children's privacy, including sending sexually explicit images to children or forcing them to view them, have increased. Additionally, there are wide variations in response times to user reports of online child sexual exploitation, as TikTok responds within 5 minutes to general content, while Discord takes 13 hours to respond to direct message reports[[14]](#footnote-14).

**Fourth: What practical recommendations do you suggest to countries, technology companies, and online service providers to prevent sexual exploitation and abuse of children in the digital environment?**

Maat sees the need for the following:

* Advocating for the establishment of a common framework and global alliance for more secure and accountable technology management, especially with regard to the management and coordination of artificial intelligence.
* Urging the United States to pass The EARN IT Act, under which technology companies based in the United States are required to report suspected digital child sexual abuse materials to law enforcement agencies.
* Setting clear and distinct boundaries between the concept of child sexual exploitation and other terms and concepts that may overlap with it, such as freedom of opinion and expression and respect for digital privacy, requiring work on establishing clear and specific global definitions for these concepts.
* Urging Meta to stop implementing end-to-end encryption technology until a mechanism is developed that can detect, report, and remove images of child sexual exploitation within encrypted messages.
* Coordination between governments and technology companies worldwide regarding reports on online child sexual exploitation provided by these companies to committees such as the National Center for Missing and Exploited Children in the United States, ensuring the submission of all cases of digital child sexual abuse, and continuous consultation on how to reduce such cases.
* Encouraging countries to join the We Protect Alliance to protect children from all forms of exploitation following UNICEF's recommendation.
* Distributing burdens among countries, especially major countries, and between major technology companies regarding the costs of detecting all cases of digital sexual assault against children, which encourages these companies to provide countries and specialized centers with all such data and attacks.
1. Tech companies must do more and do better if we are to stem the tide of online child sexual exploitation and abuse, safety, 16 October 2023, <https://tinyurl.com/mrymrr77> [↑](#footnote-ref-1)
2. The Sale and Sexual Exploitation of Children: Digital technology, unicef, 2020, <https://tinyurl.com/3a77ayux> [↑](#footnote-ref-2)
3. Analysis of the sexual threats children face online, weprotect, <https://tinyurl.com/ymh8smyz> [↑](#footnote-ref-3)
4. NCMEC Debuts New Sextortion Videos for Safer Internet Day, missingkids, 2 may 2024, <https://tinyurl.com/yshs6amm> [↑](#footnote-ref-4)
5. Estimates of childhood exposure to online sexual harms and their Risk Factors, weprotect, <https://tinyurl.com/5fv4r33s> [↑](#footnote-ref-5)
6. Ibid, <https://tinyurl.com/yshs6amm> [↑](#footnote-ref-6)
7. Child sexual abuse content growing online with AI-made images, report says, theguardian, 16 Apr 2024, <https://tinyurl.com/yc4kbvap> [↑](#footnote-ref-7)
8. Generative AI: what it is, what it doesn't have, and what it could mean for the UN, <https://www.un.org/ar/208258> [↑](#footnote-ref-8)
9. Techplatforms used by online child sexual abuse offenders, February 2024, <https://tinyurl.com/3mju8h28> [↑](#footnote-ref-9)
10. Four Ways the EARN IT Act Protects Kids Online, ijm, 2 july 2024, <https://tinyurl.com/45mvdsfe> [↑](#footnote-ref-10)
11. Ibid, <https://tinyurl.com/mrymrr77> [↑](#footnote-ref-11)
12. An International Perspective: Addressing Challenges to Protect Children’s Rights from Online Sexual Exploitation in the Digital Era, childlawinternational, 2024, <https://tinyurl.com/2skm9wsu> [↑](#footnote-ref-12)
13. Internet freedom can co-exist with child protection, hilltimes, 15 April, 2024, <https://tinyurl.com/4hm8fedw> [↑](#footnote-ref-13)
14. Ibid, <https://tinyurl.com/mrymrr77> [↑](#footnote-ref-14)