**Input for the Report of the Special Rapporteur on the sale and sexual exploitation and sexual abuse of children „Existing and Emerging Sexually Exploative Practices against Children in the Digital Environment “– information provided by Montenegro**

1. **Please provide information on how technologies are used to facilitate the sexual exploitation and abuse of children.**

**Response:**

The widespread use of information technologies facilitated various forms of sexual exploitation, including child exploatation and increased the risk of various forms of abuse. We have identified main risks such as: the use of suspicious websites and applications that offer suspicious services; sharing personal information on social networks; engaging in communication with unknown individuals; accessing suspicious or unknown links; meetings with unknown individuals with whom intimate contact has been established through information and communication technologies. One of the challenges is that children often use cyberspace without any restrictions or supervision from their legal guardians, thus their trust can be exploited for the purpose of committing this criminal act. Furthermore, the use of social networks and applications enables predators to locate children and gain easier access to them by using false identities, photos, and videos, all for the purpose of manipulation and ultimately abuse.

1. **What practical reccommendations would you propose for States, the technology industry and online service providers to prevent the sexual exploitation and abuse of children in the digital environment?**

**Response**

In order to prevent sexual exploitation and abuse of children, it is important that all states ensure all legal acts and regulations prohibiting the exploitation of children through information and communication technologies within its legislative system, as well as to ensure their enforcement and implementation. Additionally, it is necessary to conduct educational campaigns for children, their parents/guardians, as well as teachers, about sexual exploitation and abuse of children, and about safe use of digital technologies.

Furthermore, there is a need for further development and implementation of technologies for detecting content related to sexual exploitation and abuse of children. Additionally, it is necessary to ensure that all online platforms/applications, etc., have a prompt response to these criminal acts, including providing all available data regarding the perpetrator and promptly removing the problematic content, all aimed at protecting children.

These and similar recommendations should be part of a comprehensive approach to protect children from sexual exploitation and abuse, which would involve the participation of all relevant institutions.

1. **What are the remaining gaps that limits the effective implementation and application of existing laws, policies and guidelines to prevent, detect, report and protect children from sexual exploatation and sexual abuse online?**

**Response**

The rapid development of information technologies can pose a challenge for legal regulations, as they have to be constantly improved in accordance with new trends and threats. Additionally, due to the nature of the commission of the criminal offense, i.e., the fact that it is carried out using information technologies, there is a possibility of hindered cooperation among multiple countries in the fight against sexual exploitation and abuse of children.

Addressing these gaps requires coordinated efforts among states, online platforms (applications, etc.), the civil sector, and other relevant institutions, as well as continuous monitoring and implementation of policies and guidelines to ensure adequate protection of children.

1. **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?**

**Response**

Current challenges in the use of digital technologies, products, or services that hinder the work of law enforcement agencies in terms of investigating, detecting, removing materials related to online child sexual abuse, and prosecuting individuals associated with it, can be manifested in the use of:

- End-to-end encryption, which on communication platforms can hinder access for law enforcement agencies;

- Activities related to child sexual exploitation and abuse can be carried out on the dark web or via the Tor network, which makes tracking and identifying perpetrators difficult;

- When perpetrators and victims are in different countries, cooperation between law enforcement agencies may be hindered due to different legal systems and procedures;

- Technological innovations often surpass the capacities of law enforcement agencies, particularly in terms of tracking and detecting new methods of child exploitation and sexual abuse, as well as identifying new threats;

- The vast amount of data generated daily complicates the analysis and identification of relevant information related to this issue;

- Anonymity and false identities.

Overcoming these challenges requires investment in tools, education, and training for law enforcement personnel, as well as strengthening international cooperation and coordination among all relevant institutions.

1. **What technical and regulatory measures can be put in place by States, the technology industry and online service providers (legislative, regulatory, administrative, institutional and others) towards mitigating human risks associated of online child sexual exploitation and abuse, end ensuring the minimum harmonization across legal jurisdictions?**

**Response**

Countries should adopt stricter laws and regulations in order to ensure prevention and prohibition of online sexual exploitation and abuse of children, as well as specific laws relating to digital security and child protection. Special emphasis should be placed on organizing educational campaigns for children, their guardians, and teachers about safe use of information technologies. Additionally, each country must enhance cooperation with online platforms to ensure the removal of illegal and inappropriate material. Furthermore, international collaboration is crucial, as addressing these criminal acts often requires it. These and similar measures will be useful for creating safer environment for children in the virtual world.

1. **Are there any other practical examples of internal monitoring, complaint and reporting processes; establishment of regulatory bodies and interventions; remedial pathways; robust safeguarding procedures; children’s rights’ due diligence and risk assesments; and technical standard-setting processes to ensure safety and inclusivity by design?**

**Response**

In Montenegro, all resources of law enforcement agencies, as well as other governmental and non-governmental institutions and organizations, are fully dedicated and prepared to adequately and promptly respond in order to ensure complete protection, rehabilitation, and socialization of children identified as victims of sexual exploitation and abuse.

1. **In the case of generative Artificial Intelligence and end-to-end encryption, what are the challenges and recommended mitigation measures, including the application of advanced technology needed by technology companies, online service providers and law enforcement to prevent blocking the sharing and removal of CSAM?**

**Response**

Generative artificial intelligence and end-to-end encryption pose challenges in preventing the sharing and removal of Child Sexual Abuse Material (CSAM), as they hinder the tracking and identification of content related to sexual exploitation and abuse of children. One possible way to mitigate these challenges is through the development of advanced technologies that can automatically detect and filter questionable material. Additionally, increasing cooperation between states and companies is crucial to preventively act and reduce the likelihood of children being exposed to sexual exploitation.

1. **Are there any examples of proactive measures taken to facilitate consultation and participation with a broad range of stakeholdres, including children and child-rights organisations, for informing policy and legislation, setting technical standards and implementing processes to eradicate child sexual abuse and exploitation in the digital environment?**

**Response**

Montenegro has recognized the importance of proactive action, which is primarily reflected in launching discussions with children, active cooperation with civil sector, conducting research and analysis, education and training. Accordingly, officers of the High-Tech Crime Prevention Group, in cooperation with UNICEF in Montenegro, are coordinating a research project called Disrupting Harm (Protection from Violence), which aims to collect evidence of sexual exploitation and abuse of children on the Internet. This research will be conducted by the research team ECPAT International, INTERPOL and UNICEF Innocenti - Global Office for Research and Projections - in cooperation with national partners. Also, Montenegro is one of the participants in the pilot project, which is planned to be implemented in 2025, and refers to the H4U platform.

1. **What kind of mechanism could be put in place to best support and coordinate the joint public and private industry participation at the international level on existing threats that digital techonologies pose to children in order to ensure harmonisation and mainstreaming across domestic and regional efforts when combating this phenomenon?**

**Response**

In order to ensure effective support and coordination of the public and private sectors at the international level in the fight against digital threats to children, we truly believe that it would be necessary to establish an international coordination center or a network of organizations that would be dedicated to the analysis, monitoring and adequate response to this type of threats. The aforementioned could ensure a quick exchange of information between state institutions, private companies, and non-governmental organizations, with the aim of monitoring new phenomena and developing adequate strategies to combat them. Additionally, it will be useful to initiate educative campaigns for children about the safe use of digital technologies and promoting awareness of cyber security.