

Mister Chair, distinguished participants, dear colleagues,

My name is Ioana Bauer and I am here representing eLiberare, a CSO fighting against human trafficking and for the protection of those affected by the phenomenon. I want to thank you for the opportunity to present data from the field and concerns raised not only by the third sector, but also by law enforcement that we collaborate with.

After 2020, business as usual took on a very different meaning. As lockdowns were imposed around the globe, what started emerging weren't only the new challenges brought about by the COVID19 pandemic, but also the deepening of the already existing gaps and faults within our systems. All of a sudden, in a lot of areas, we all got to experience what the emperor's new clothes actually looked like.

This was definitely the case for the internet and communication technology field, when everything moved online, including the expansion of technology-facilitated trafficking in human beings. When everyone was adapting, so did the business model of human traffickers who rapidly moved their operations online via misuse of technology. If before, the internet was mostly a means of recruitment, now we see it at every stage of human trafficking: in grooming, in controlling and coercion, and in exploitation.

While I do not think there is anyone challenging the gravity of cyber sexual abuse and exploitation, I do think that we are still struggling to grasp the scale of it. In 2021, there were more than 29 million reports of CSA globally, representing a 38% increase from 2020 - that means 85 million images and videos (up from 65 million in 2020). We have seen operations that exposed offender rings with as many as 400,000 members lurking behind the anonymity of a username that could be created with little to no verification.

I believe this is reason enough to start thinking about how to include mandatory reporting for technology facilitated trafficking and exploitation. We have witnessed over the years that the principle of zero responsibility for monitoring third party content, linked with self-regulation, has not created the results we have been hoping for. The scarce standards for the industry, the lack of application of voluntary principles, no incentives for compliance are all part of this anomaly. The safety of children and vulnerable adults is not an issue we should leave in the realm of hope!

And while monitoring online content is directly challenged by privacy restrictions and encryption, this does not mean that we cannot proactively think about prevention of harm. A few simple examples include mandatory age verification for the individuals depicted in uploaded material, for individuals uploading material, and for individuals viewing such material. Also, we cannot imagine taking out the need for consent in the physical realm, so why do we think that consent verification online for any sexually explicit content distributed via ICT is not as vital?

Harmful and prohibited content directly linked to human trafficking and exploitation, especially that of children, must bring with itself liability and an obligation of removal, as well as the option for law enforcement or magistrates to block online platforms that continuously go against these rules.

Ambiguity is the enemy of protecting our children and those most vulnerable in our world. We saw how lack of clarity led to a six-months period in 2021 where companies stopped reporting child sexual abuse material for fear of breaking privacy regulations introduced at the end of 2020. We need clear indicators for both compliance, and its lack thereof.

We heard yesterday the need for clear definitions. It is the same with the crime of human trafficking and exploitation in the online realm. There are concerns that the legal definition of trafficking, as stated in the Palermo Protocol, might not be fitting for technology facilitated trafficking, thus causing an obstacle for identification of victims and their access to services and justice.

Several bodies, such as the OSCE and the Council of Europe, as well as my previous copanelists, have warned about the lack of consensus on how law enforcement, policymakers and magistrates should treat evidence gathered by an AI system, highlighting the need for clear policy guidance in criminal justice proceedings. There is a need for regulatory frameworks governing the collection and use of digital evidence, and it is time to assess if the premise of voluntary data sharing in the crime of tech-facilitated human trafficking and exploitation is enough.

We do not want traffickers to escape justice. We do not want to contribute to the already existing culture of impunity because we do not have clear references to technology facilitated trafficking in human beings. Let's not forget that we now build on both the Budapest Convention and the Lanzarote Convention which emphasize the need for procedural reform enabling effective investigation and prosecution of cyber sexual exploitation. However, neither of these conventions cover the crime of human trafficking exhaustively: the Budapest Convention does not expressly reference THB at all, and the Lanzarote Convention only applies to the exploitation of children, and not that of adults.

We represent here a very diverse group, with very different tools and skills. I am thankful for colleagues such as the team from the GI, present in the room with you now, or Child 10, who focus entire programs on the issue and with whom we will continue to contribute with our expertise and firsthand experience on this, and while we all face different challenges, we also all share a common responsibility to protect children and those most vulnerable. I hope we will use this opportunity to do exactly that.