Vilnius University Press

Contents lists available at Vilnius University Press

Teisė
2024, vol. 132, pp. 145–155

ISSN 1392-1274 eISSN 2424-6050
DOI: https://doi.org/10.15388/Teise.2024.132.11

Strategies for Intervention and Prevention in Online Child Sexual Exploitation

Muhammad Imran Ali LL.M.

https://orcid.org/0000-0003-1395-229X
Principal
Quaid-e-Azam Law College Kasur, Pakistan
E-mail: principal.kasur@qlc.edu.pk

Strategies for Intervention and Prevention in Online Child Sexual Exploitation

Muhammad Imran Ali LL.M.

(Quaid-e-Azam Law College Kasur (Pakistan))

Summary. *Online child sexual exploitation* (OCSE) is a significant societal and technological problem that ought to be addressed immediately. This article broadly deals with the intricate complexity of OCSE, laying bare the identities and behaviors of online predators, the characteristics of virtual playgrounds, and the adverse consequences for victims. Virtual offenders, by taking advantage of the anonymity of internet spaces, mostly use a variety of tactics to approach vulnerable children. These tactics demand thorough assessment to work out and deliver effective interventions. Virtual environments, such as game communities and chat rooms, have become the perfect hunting grounds for predators, which accentuates the crucial need for preventive measures. Nonetheless, technology gives reason for optimism about the elimination of OCSE despite the challenges of scale and precision. This article, therefore, conducts an in-depth analysis of the issue of online child sexual exploitation and offers comprehensive interventions as a way of increasing knowledge and mobilizing action to shield children from online child sexual exploitation.
Keywords: Cyber predators, laws, online child sexual exploitation, technology, virtual playgrounds.

Internetinio vaikų seksualinio išnaudojimo intervencijos ir prevencijos strategijos

Muhammad Imran Ali LL.M.

(Privatus universitetas, Lahoras, Pakistanas))

Santrauka. Internetinis vaikų seksualinis išnaudojimas (angl. OCSE) yra svarbi visuomenės ir technologijų naudojimo problema, kurią reikia nedelsiant spręsti. Šiame straipsnyje plačiai nagrinėjamas kovos su šiuo reiškiniu sudėtingumas, atskleidžiama vadinamųjų kibernetinių plėšrūnų tapatybė ir elgesys, virtualių žaidimų aikštelių ypatybės ir neigiami padariniai seksualinio išnaudojimo aukoms. Virtualūs nusikaltėliai, pasinaudodami interneto erdvių anonimiškumu, dažniausiai taiko įvairias taktikas kreiptis į pažeidžiamus vaikus, o tai reikia kruopščiai įvertinti, kad intervencija taptų veiksminga. Virtuali aplinka, tokia kaip žaidimų bendruomenės ir pokalbių kambariai, tapo puiki kibernetinių plėšrūnų medžioklės vieta, todėl pabrėžtinas esminis prevencinių priemonių poreikis. Nepaisant to, nepaisant masto ir tikslumo iššūkių, technologijos duoda pagrindo optimizmui dėl OCSE panaikinimo. Todėl šiame straipsnyje išsamiai analizuojama vaikų seksualinio išnaudojimo internete problema ir siūlomos įvairios intervencijos kaip būdas didinti žinias ir sutelkti veiksmus siekiant apsaugoti vaikus nuo seksualinio išnaudojimo internete.
Pagrindiniai žodžiai: kibernetiniai plėšrūnai, įstatymai, internetinis vaikų seksualinis išnaudojimas, technologijos, virtualios žaidimų aikštelės.

Received: 06/04/2024. **Accepted:** 26/06/2024

Introduction

It is very hard to overstate the numerous and alarming incidents of *online child sexual exploitation* (OCSE), which is a very sensitive and acute social problem, as well as a tech challenge. This article undertakes to fully capture the phenomenon of the sexual abuse of minors in the cyber world by explaining who the cyber predators are, what virtual playgrounds look like, how the victims are affected, how legal and ethical questions arise, how technological solutions should be used, and what strategies for preventing this crime can be adopted. Virtual offenders have modified their approaches, strategies, and motivations which enable them to prevail within the context of hesitation and anonymity in the internet spaces. These people, ranging from those who seek pleasure from illegal sexual desires to those who pursue financial gain, leverage the convenience of the communication devices to target at-risk children (Jeglic et al., 2023, p. 8). The key lies in understanding the complexity of their behavior, which enables the development of effective interventions and the protection of potential victims.

The virtual playgrounds, which are basically web-based media platforms, the virtual gaming communities (Sirola et al., 2021, p. 172), and the chat rooms act as the ideal cauldrons for the proliferation of online child sexual exploitation. These locations offer predators vast and uninhibited possibilities for communicating and interacting with minors, which eventually leads to their seduction, manipulation, and abuse. Imposters assume such functions as grooming minors, which is done with much ease. While the development of virtual playgrounds is a good step in innovation, it also points out the potential use of technology by predators as a tool to exploit and abuse (Quayle, 2020, p. 437). Therefore, the implementation of preventive measures to cut risks becomes an urgent matter.

The developed countries will probably face legal and ethical difficulties in upholding the matter of online child sexual exploitation just because the issue is highly complicated. Given the current topic of jurisdiction, privacy issues, and constant pressure against expression and child protection, it will not be easy to find a solution (Witting, 2021, p. 746). Bolstering children's safety is critical, and it requires high-level approaches for finding solutions and communication with all stakeholders.

Technological advancement is currently the main means to stop OCSE, but there are many other issues associated with this approach. AI-enabled technology for monitoring the content and user identification through blockchains along with other upcoming developments might open a door for approaching abusive acts (Kalenzi, 2022, p. 6). However, these technologies have scalability problems, precision issues, and flexibility, which are to always be reconsidered as joint efforts involving tech gurus, policymakers, and activists.

The intersection of technology and online child sexual exploitation is marked by the combination of the two factors, which calls for a subsequent connotative solution consisting of many elements. Through the investigation of cyber predators, digital playgrounds, and victim impacts, along with legal and ethical issues, technological solutions, and protective measures, we move closer to building up a more comprehensive counteraction scheme. Collaboration between players ranging from policymakers to scientists, legislators and ethicists based on quantifiable evidence and the code of ethics is the best way to protect children from internet-related risks (Jeglic et al., 2023, p. 2).

A qualitative method that is supported by a literature review is adopted in this article. The analysis of quantitative data derived from a number of sources, such as academic journals, reports, and legislation, is the main starting point of the article as it looks into the behaviors of cyber predators, the dynamics of virtual playgrounds, and, finally, the impact on the victims.

1. Online Child Sexual Exploitation

Online child sexual exploitation (OCSE) institutes, detects, and exposes the devastating face of cybercrime as it is driven by the social media and internet abuse, which is prevalent in our present online spaces. Such despicable behavior comprises various sorts of norms, such as grooming, coercing, and sharing of *child sexual exploitation material* (CSEM) (Victoria, 2019, p. 209). One of the subtlest but most dramatic features of OCSE is the location and the acquisition of available anonymity through the use of the internet, allowing perpetrators to behave with a kind of impunity and reach out to victims from all parts of the world. This is exemplified by the fact that certain grooming activities, where the online predators create trust with minors and sexually exploit them, have evolved with the changing technology which now helps the predators join social media networks and other online platforms that are often used by children (Jeglic et al., 2023, p. 3). The emergence of encrypted messaging apps, on the other hand, adds an extra complication to the role of law enforcement because such platforms offer secure communication channels where offenders can exchange illicit content and code-coordinate each other's activities without trace. In a similar vein, the elasticity of the child sexual abuse content gives rise to the dark web market, which, in turn, fosters a thriving underground market where child exploitation persists (Woodhams et al., 2021, p. 7). However, taking into account the legal situation, joint action and cooperation across various countries is difficult. Besides, technology changes at a great speed, demanding companies to continuously align their strategies with the new threats that stem from this technology development. Whereas legislative measures and technological tools may offer great assistance in the course of overcoming this issue, the common strategic approach has to start with the prevention level of the issue (Federico et al., 2020, p. 718).

2. Relationship Between Technology and Online Child Sexual Exploitation

The merging of technology and online child sexual exploitation (OCSE) gives rise to a very complicated and manifold problem which forms the global nature of the issue, requiring coordinated efforts on the international level. In different countries, there can be different socio-cultural contexts, legal frameworks, and technological landscapes, and they can affect the figures of OCSE within a certain geographical space. To illustrate, in countries with advanced Internet infrastructure, like the United States and the United Kingdom, the broad usage of the Internet and the high levels of digital connectivity have aided the surge of OCSE on platforms such as social media, online gaming, and file sharing networks. Notably, the *Operation Rescue* in the US (Haggerty, 1993, p. 53) and the *National Crime Agency* investigations in the UK have brought to the limelight the OCSE networks in these countries and, therefore, show the need for effective law enforcement with the collaboration with tech companies to put an end to the proliferation of this crime (Hillman et al., 2014, p. 692).

Alternatively, in the more developed nations, where the internet is universally available and the regulation is better, OCSE demonstrates differently from that in the developing nations where poverty, illiteracy, and child protection infrastructure are lacking. India and Pakistan have been the main destinations for OCSE as a result of the widespread use of affordable smartphones and the growth of internet penetration, which has left more children vulnerable to local and foreign criminals. The OCSE case of the *Dark Web Paedophile Platform* (Woodhams et al., 2021, p. 7), exposed recently in India, hints at the global dimension of OCSE and the difficulties that law enforcement agencies confront in trying to defend against well-hidden online networks that transcend territories. The *Kasur Child Sexual Abuse Video Case* in Pakistan was all about tormenting and threatening almost 280 innocent children

(Ali, 2015, p. 101). However, international cooperation involving information exchange is still crucial in order to combat the global threat of the global outbreak of OCSE. International bodies, such as INTERPOL (Calcara, 2020, p. 534) and the Virtual Global Taskforce, utilize cross-border cooperation as a crucial tool to disrupt networks and liberate victims worldwide.

3. Deciphering Cyber Predators

Cyber predators are one of the most diverse threats to internet security, especially because of the wide-spreading challenges of online child sexual exploitation (OCSE). Identification of who, how, and why is involved is an essential step in the solution of this ever-spreading problem (Roche et al., 2023). Such predators show different characteristics and examples from different countries; they are a mirror of all kinds of socio-cultural contexts, legal frameworks, and technological infrastructures.

Primarily, the offenders' online profiles are profoundly different. On the one hand, some of them conform to the image of loners and misanthropes, while, in spite of that, the other part, like everyone else, enjoys social interaction. A great many online offenders occupy roles of confidence and trust, for instance: teachers, pastors, or law enforcers. An example of this would be Mark Frost from the UK (BBC News, 2017), a former police officer who used to access the indecent images of children surreptitiously via his position, which shows how complicated the identification of these potential predators can be.

Likewise, cyber pedophiles employ different strategies to take advantage of those children who are involved in online activities. These techniques generally use a combination of manipulation, deception, and coercion strategies. In this context, an example is the creation of fake identities or the gradual grooming of their victims over an extended period to inoculate them from maladaptive behavior (Joleby et al., 2021). In some instances, predators exploit the more refined hacking techniques that assist them in stealing personal information or bypassing security measures. A sample approach of cyber predators using a variety of methods to exploit children online from the United States is one instance. Not so long ago, in 2019, the case of *Operation Broken Heart* shed light on the wide use of online profiles and complex social engineering strategies by the predators (Nhan, Bowen, 2020, p. 5).

Moreover, the reasons why cyber predators perform their criminal actions are characteristically multifarious and complicated. Perverted sexual impulses or a mental illness drive some people's actions, while money or power dynamics drive others. On other occasions, it is not so uncommon for organized gangs to get involved in OCSE activities for earning money, and, in some nations, children from deprived social backgrounds are abused for this purpose. In addition, the fact that the internet offers full anonymity can turn non-criminals into people ready to break any law and be immune in the effort to stop online exploitation. The legislation addressing online child sexual abuse exploitation could be different from each other in terms of their region-specific response protocols and relative performance. Some of the judicial systems have adopted tougher laws and regulations to identify and catch the culprits as well as protect the children, while other jurisdictions are yet to even implement laws or amend the existing ones so that they go along with the high rate of changing technologies. An example of this is the *General Data Protection Regulation* (GDPR), which the EU has developed to save data (Hoofnagle et al., 2019, p. 78). Consequently, with these stringent data protection policies, dealing with digital surveillance has become more complicated.

4. Virtual Playgrounds Enabling Online Child Sexual Exploitation

Virtual playgrounds, including online gaming platforms, social media apps, virtual worlds, forums, live streaming broadcasts, and encrypted messaging services, are the stage for the worst crimes of them all, such as the sexual exploitation of children on the internet (OCSE). Online platforms offering anonymity and interactivity are characteristic of effective abusers and online scammers who mislead children with the aim of gaining their trust (Jain et al., 2021, p. 2165). Cumulatively, these risks portray a scenario in which a complete plan is needed to address the issue of the vulnerable individuals' protection.

The major online gaming platforms work as a virtual playground where children socialize and interact with other people in real time. The predators use voice and text chat to become close friends with the young players and subsequently direct them to do inappropriate actions (Marsh, 2010, p. 31). In the US, where the major online gaming platforms include *Fortnite*, *Roblox*, and *Minecraft*, children's modes may or may not feature real-time interaction (Rustadet et al., 2024, p. 300). On the other hand, the predators take advantage of features such as voice and text chat to get close to the young players by pretending to be another gamer and engaging in improper activities, thereby accelerating the need for safety measures and parents' careful watchfulness. Nor can social platforms with age restrictions and privacy be free of exploitation. Sex offenders will infiltrate children's social circles by using fake profiles as a way to access them and, ultimately abuse them sexually.

Internet trolls and cyber predators may choose online forums and virtual worlds as alternatives in their pursuit to put children at risk. These environments provide cover as the peruses are hidden, whereas they prey on the unaware victims. Examples such as violence on the *Second Life* platform and others show the strong interdependence between technology and harassment (Fiolet et al., 2021). As a result, the children are venturing into live streaming platforms, which could potentially expose their personal information to exploitation. Scammers might use and take advantage of vulnerable people who cannot protect themselves and whom they befriend by using some type of umbrella, such as mentorship or friendship. The filtering and protection of these platforms are becoming difficult for moderators and regulators because the offenders are now easily streaming these bad activities or events, and doing so makes them very difficult to trace and prevent (Lavorgna et al., 2023, p. 1051).

Addressing the challenges connected with tech companies, law enforcement agencies, and civic organizations calls for coordination among all the players. High-end content regulation and the application of illegality detection techniques will put a stop to the distribution of unlawful content on online platforms (Stasi, 2019, p. 103). Recently, development technologies gave us virtual worlds. On the one hand, they are a place to socialize and entertain, but, on the other hand, they can be a risk for OCSE.

5. Legal Considerations in Addressing Online Child Sexual Exploitation

The concept of Law as a contributor to children's protection in the digital age has turned out to be one of the most significant points because of which we should make children safe. By recognizing the continuous development of technology, criminals are provided with new methods of committing crimes; thus, the law has to be upgraded to allow the prosecution of such crimes. The advantage of the internet, as it is borderless, creates complications for the selection of laws which would tackle global cyber offences that concern several jurisdictions. The USA has enacted the *PROTECT Our Children Act* (PROTECT Our Children Act, 2008), which is about child exploitation, including online issues pertaining to the sexual abuse of children. Through this Act, funding is allocated to law enforcement agencies for the investigation and apprehension of such crimes, and a National Internet Crimes Against

Children Data System has been established for this nation-wide sharing of information. In the UK, the *Sexual Offences Act* (Sexual Offences Act, 2003) stipulates that online grooming, as well as the possession, distribution, and production of indecent images of children, is criminalized. This is another preventive measure that helps protect children against the negative consequences of online sexual predators. Australia's *Criminal Code Amendment (Protecting Minors Online) Act* (Criminal Code Amendment (Protecting Minors Online) Act, 2017), also called *Carly's Law*, addresses the issue of the use of electronic communication for the purpose and with the result of exploiting minors sexually or sexually abusing them. Therefore, we need to implement laws that would encompass both prevention and punishment. Prevention implies a broad scope consisting of education, campaigns, techniques, and anything else that can decrease the child's palatability to such an outcome. For instance, social media platforms can utilize age verification mechanisms to prevent children from being exposed to explicit content, whereas filtering software can block them. In the UK, the *Digital Economy Act* (Digital Economy Act, 2017), as it stands, is focused on the protection of children online, and this is evidenced by Part 3 that comes with the Act and requires age verification for pornography that is watched online. This Act compels pornographers to have stringent measures that stop children from accessing porn. Besides this new Act, the legislation makes an appeal to Internet providers to avail of existing software filters in the marketplace, which have to restrict exposure to reproachable content. In Australia, the *Online Safety Act* (Online Safety Act 2021), among others, makes it a misdemeanor to share intimate photos without the consent of the other party and makes it easier to have the undesirable material removed. The government is also on the front lines of online security, just like the *eSafety Commissioner*, which is an educational and awareness program to guarantee that all children, parents, and educators have the knowledge and skills that can assist them in dealing with the risks connected to the Internet.

Moreover, providing a safe haven for the victims and witnesses is the most crucial task of any legal system. The children who are subjected to the crime of OCSE run a high risk of experiencing trauma, and they need to receive thorough care from the specialists and counsellors. In the US, a number of Children's Advocacy Centers (CACs) are funded by the *Victims of Child Abuse Act* (VOCAA) (Victims of Child Abuse Act, 2022) which are specifically designed for handling OCSE. Under the *Victims' Rights and Restitution Act* (Victims' Rights and Restitution Act, 1990), victims can have an opportunity to become part of the legal proceedings and be able to testify through closed hearings and video testimony if they cannot be present in court at all to avoid re-traumatization. In the UK, the *Youth Justice and Criminal Evidence Act* (Youth Justice and Criminal Evidence Act, 1999) offers special qualifications, such as the use of video testimony, either live or recorded, to young witnesses and requires services such as Childline and NSPCC. It is the Evidence laws in Australia that allow for special court measures to protect vulnerable witnesses, by utilizing organizations such as Bravehearts and ACCCE for counseling and rehabilitation, thereby aiding the victims to suffer less and to live in society in a more integrated way (Fairclough, 2021, 1087).

Legislative frameworks, specifically designed to upgrade technology and keep up with the growing dangers, also receive attention. Regarding the United States, it is the *EARN IT Act* (EARN IT Act, 2023), which targets shielding children from online harm and preventing online sexual abuse. It is considered a useful instrument to provide the kind of security for children or the electronic safety people in households rely on. In the meantime, the UK's *Investigatory Powers Act* (Investigatory Powers Act, 2016) has such functions as: ISP tracking of web site visit histories; and provision of surveillance and interception of the telecommunications' part. The Act also provides the authorities with the right to install monitoring devices on people's computers. Besides, the *Crime (Overseas Production Orders) Act* (Crime (Overseas Production Orders) Act, 2019) broadened its subject to cover the gain of electronic

information for the investigation of a serious crime of OCSE from foreign service providers. In addition, *The Assistance and Access Act* of Australia (The Assistance and Access Act, 2018) allows authorities to force tech companies to disclose their encryption codes; thereby, this measure is not appreciated in terms of privacy and cybersecurity protection.

6. Challenges to Technological Solutions in Addressing Online Child Sexual Exploitation

The task of detecting and removing illegal content on online media is fairly challenging due to the amount of the user-generated content. Artificial intelligence and machine learning now play vital roles in handing over the whole content moderation process to the machines. Platforms such as *Facebook* and *YouTube* use AI technology in order to preemptively flag and eliminate content containing child sexual exploitation material (CSEM) (Grandinetti, 2023, p. 1281). In the United States, tech giants such as *Facebook*, *Google*, *YouTube*, and *Microsoft* invest into systems based on AI-driven tools to come against OCSE. Machine learning algorithms are used that can detect and block illegal content, and NCMEC is one of the organizations that supports this development. In the United Kingdom, the partnership of the Government with companies in the tech field, including the *Internet Watch Foundation* (IWF), relies on the help of AI to find and remove CSEM. The *eSafety Commissioner* of Australia uses AI tools to deal with the content of explicit nature by increasing international partnerships to make efforts on a global scale. Internet anonymity in fact plays an important role in the perpetrators hiding. Technologies such as VPNs and Tor networks allow one to maintain their anonymity online, and law-enforcing agencies are unable to identify these offenders (Jardinea et al., 2020, p. 31719). Blockchain technology, which uses a decentralized and pseudonymous manner to store and cryptographically hash information, proposes more difficulties in identifying participants if they are involved in CSEM exchanges or payments for illegal services (Habib, 2022, p. 15). While enforcement authorities in the US, UK, and Australia meet the challenge of hunting the disseminators of OCSE, at the same time, they encounter difficult circumstances due to the availability of VPN and Tor networks. These technologies leave traces, allowing criminals to hide their identities by remaining untraceable during investigations.

The constant change witnessed in online platforms necessitates periodic reviews of the technology solutions in use. Pursuers are more and more prone to exploiting new possibilities and vectors, which means that authorities and tech businesses have to maintain digital agility and innovation. As a case in point, the live-streaming platforms fuel up the live sexual abuse of children, which quickly demands state-of-the-art tools to recognize, intercept, and stop such streams (Drejer, 2024, p. 267). Technologies of human identification, for instance, face recognition and age verification algorithms, unveil the issues regarding privacy, consent, and exploitation that could take place, such as the implementation of facial recognition techniques in public places, for example, to identify missing children. Consequently, we need to have a debate about the privacy and anonymity rights of individuals that may be at odds with security, which is the driving force behind the advancement of such technology (Raposo, 2023, p. 527). In the US, the use of biometric identification, such as facial recognition, in trying to stop child sexual exploitation has been the focus of ongoing debates and, sometimes, ethical issues. Organizations such as the *American Civil Liberties Union* (ACLU) have a role in promoting a strict legal framework that safeguards privacy, thereby ensuring that exposures such as the facial recognition technology are used for identifying the missing children. Similarly, in the UK, the use of facial recognition and age estimation algorithms for combatting child sexual exploitation faces such ethical difficulties at the national level. Civil society organizations like *Privacy International* are the watchdogs over efforts

by the governments to deploy facial recognition systems in public areas to ensure that privacy presumptions are adhered to, and that accountability and transparency are maintained. In Australia, chats related to tech adoption for dealing with OCSE comprise many stakeholders, including Government departments, privacy advocates, and tech firms. For example, the *Office of the Australian Information Commissioner* (OAIC) promotes consultation and policy development among organizations that use biometric identification approaches, as well as attention to privacy issues and ethics.

7. Legislative and Technological Preventive Strategies for Safeguarding Children from Online Sexual Exploitation

In preventing online child sexual exploitation, legal frameworks are vital as a means to protect children from the threat of virtual encroachment. The development of jurisdictional definitions is important given the borderless nature of the internet, and, due to that, it complicates the enforcement of laws across multiple jurisdictions. For example, enacting laws such as the *PROTECT Our Children Act* in the US and the *Sexual Offences Act* in the UK by allocating resources for investigation and prosecution are devices often used to take care of these crimes. Australia has passed the *Criminal Code Amendment Act* (Carly's Law) concerning online child sexual exploitation by imposing penalties on immoral actions involving children. Moreover, legal frameworks have to include prevention along with punishment for the crime. Education, awareness campaigns, and technology imply this, which helps children be less susceptible to risks and evil. For instance, the *Digital Economy Act* in the UK has made age verification for online porn content a legal requirement, and the *Enhancing Online Safety Act* in Australia criminalizes the distribution of spiteful sexual images. These provisions, besides the project of the *eSafety Commissioner* in the light of raising awareness, are campaigning to restrict the minors' access to harmful content.

Moreover, the protection of victims and witnesses must be a positive consideration. Children-victims who are involved in proceedings require due diligence as concerns the procedures adopted, including specialized courts for children or procedures to avoid re-traumatization. Laws like the *Victims of Child Abuse Act* in the US and the *Youth Justice and Criminal Evidence Act* in the UK, respectively, give out support services and encourage the victims' participation in the legal system. Legislation such as, for instance, the *EARN IT Act* in the US and the *Investigatory Powers Act* in the UK, is focused on the overall internet safety without undermining the privacy concerns.

Solutions are also of great value when it comes to fighting child sexual exploitation online because of the technology behind it. Artificial intelligence helps in the content moderation of *Instagram* and *YouTube*, although concerns of overcensorship are still being expressed. For instance, the emergence of virtual private networks (VPNs) and Tor network services reduces the chances of an investigator coming closer to a perpetrator; thus, advanced strategies should be developed and put in place.

Furthermore, the ethical use of technology requires attention. Biometric identification methods raise the privacy question; therefore, the appropriate regulations have to be in place to ensure that people are not infringed on. While the United States, UK and Australia are just a handful of nations wrestling with the efficacy of these technologies against the privacy standards, the essence of the conversation still revolves around striking the right balance. Eventually, to achieve this goal, different strategies that are legally, technically, and ethically based must be satisfied. Legal frameworks are strengthened when they are exposed to technological advancements. Moreover, the right ways of using the internet are promoted if ethical use is maintained. Thus, societies can aspire to have a safer digital environment for children globally.

Conclusions

Online child sexual exploitation (OCSE) is the result of the combined forces of technology, humane behavior, and legal processes. Exploring areas such as profile identification, tactic comprehension, and motivational analysis of cyber predators is essential for creating robust prevention and intervention strategies. Technology is in a state of constant evolution, and the platforms for such crimes also advance, thus presenting an arena where the abusers hide and take advantage of the defenseless children. The legal framework for OCSE is complex, necessitating a holistic approach which would ensure the protection of children while at the same time safeguarding digital freedoms. However, as much as the digital society is rapidly changing, it constantly demands some innovations, technological solutions and interventions which would be there to help. AI-enabled moderation, blockchain-assisted identity verification, and others are among the innovative approaches to combatting online child sexual exploitation. But it is a must to implement these solutions carefully, letting them be well thought out for unwarranted consequences and an ethical framework.

Prevention is still the very foundation of such efforts to protect children online. Empowerment of the children with digital literacy skills, open communication with the parents, and promotion of an online safety culture are core elements in any prevention of online abuses and harms. Nevertheless, the miraculous bullet-like solution is not a good one that is fit for the purpose. Rather, implementation of a comprehensive system consisting of legal, technological, and social elements is required for the complete cancellation of OCSE. Thus, the sensitization of society, an improved regulation, adoption of technology, and joint efforts would be the pillars in the creation of a child-safe global online environment.

The struggle against OCSE must be a worldwide, joint and universal effort of all of the society's components. It calls for undivided attention, a high level of innovation, and faithful care of children's rights and general health. With the growing complexity of the digital era, we must remain careful and keep in mind that every member of society is vulnerable to engaging in inappropriate activities. Therefore, a world in which every child is safe from online sexual exploitation must be created. If we have a community spirit, we can achieve the same. It will help us create a better digital world that is safe and hospitable for future generations.

List of Sources

Legal acts

US Laws, EARN IT Act, S. 1207, (2023).
US Laws, Victims of Child Abuse Act, (2022).
US Laws, PROTECT Our Children Act (2008), Pub. L. No. 110-401, 122 Stat. 4229.
US Law, Victim's Rights and Restitution Act of (1990), Pub. L. No. 101-647, 104 Stat. 4789.
UK Public General Acts, Sexual Offences Act (2003), c. 42.
UK Public General Acts, Crime (Overseas Production Orders) Act (2019), c. 5.
UK Public General Acts, Digital Economy Act (2017), c. 30.
UK Public General Acts, Investigatory Powers Act (2016), c. 25.
UK Public General Acts, Youth Justice and Criminal Evidence Act (1999), c. 23.
Australia Acts, Online Safety Act, C2022C00052 (C01) (2021).
Australia Acts, The Assistance and Access Act (2018).
Australia Acts, Criminal Code Amendment (Protecting Minors Online) Act (No. 50, 2017)

Special literature

Ali, A. (2015). Kasur Child Sexual Abuse Case. *Pakistan Journal of Applied Social Sciences, 2,* 101–104, http://dx.doi.org/10.46568/pjass.v2i1.288

Calcara, G. (2020). A Transnational Police Network Cooperating Up to the Limits of the Law: Examination of the Origin of INTERPOL. *Transnational Legal Theory, 11(4),* 521–548, https://doi.org/10.1080/20414005.2020.1793282

Drejer, C., Riegler, M. A., Halvorsen, P., Johnson, M. S. & Baugerud, G. A. (2024). Livestreaming Technology and Online Child Sexual Exploitation and Abuse: A Scoping Review. *Trauma, Violence, & Abuse, 25(1),* 260–274, https://doi.org/10.1177/15248380221147564

Fairclough, S. (2021). The Lost Leg of the Youth Justice and Criminal Evidence Act (1999): Special Measures and Humane Treatment. *Oxford Journal of Legal Studies, 41(4),* 1066–1095, https://doi.org/10.1093/ojls/gqab014

Federico Brunetti *et al*. (2020). Digital Transformation Challenges: Strategies Emerging from a Multi-Stakeholder Approach. *The TQM Journal, 32(4),* 697–724, https://doi.org/10.1108/TQM-12-2019-0309

Fiolet, R., Brown, C., Wellington, M., Bentley, K. & Hegarty, K. (2021). Exploring the Impact of Technology-Facilitated Abuse and Its Relationship with Domestic Violence: *A Qualitative Study on Experts' Perceptions. Global Qualitative Nursing Research, 8.* doi:10.1177/23333936211028176

Grandinetti, J. (2023). Examining embedded apparatuses of AI in Facebook and TikTok. *AI Society, 38,* 1273–1286.

Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S. & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet, 14*(11), 1–22. https://doi.org/10.3390/fi14110341

Haggerty DF. (1993). Operation Rescue: What Legacy of Disobedience? *The Linacre Quarterly, 60(4),* 50–58.

Henry Hillman, Christopher Hooper, Kim-Kwang Raymond Choo. (2014). Online Child Exploitation: Challenges and Future Research Directions. *Computer Law & Security Review, 30(6),* 687–698, https://doi.org/10.1016/j.clsr.2014.09.007

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What It is and What It Means. *Information & Communications Technology Law, 28*(1), 65–98, https://doi.org/10.1080/13600834.2019.1573501

Jain, A. K., Sahoo, S. R. & Kaubiyal, J. (2021). Online Social Networks Security and Privacy: Comprehensive Review and aAnalysis. *Complex Intelligent Systems, 7,* 2157–2177.

Jardinea, E., Lindnerb, A. M. & Owenson, G. (2020). The Potential Harms of the Tor Anonymity Network Cluster Disproportionately in Free Countries. *Proceedings of the National Academy of Sciences of the United States of America, 117(50),* 31716–31721.

Jeglic, Elizabeth L. and Georgia M. Winters. (2023). The Role of Technology in the Perpetration of Childhood Sexual Abuse: The Importance of Considering Both In-Person and Online Interactions. *Children 10(8).* https://doi.org/10.3390/children10081306

Joleby, M., Lunde, C., Landström, S. & Jonsson, L. S. (2021). Offender Strategies for Engaging Children in Online Sexual Activity. *Child Abuse & Neglect, 120.* https://doi.org/10.1016/j.chiabu.2021.105214

Kalenzi, C. (2022). Artificial Intelligence and Blockchain: How Should Emerging Technologies Be Governed? *Frontiers in Research Metrics and Analytics 7.* https://doi.org/10.3389/frma.2022.801549

Lavorgna, A., Tartari, M. & Ugwudike, P. (2023). Criminogenic and Harm-Enabling Features of Social Media Platforms: The Case of Sharenting Practices. *European Journal of Criminology, 20(3),* 1037–1060, https://doi.org/10.1177/14773708221131659

Marsh, J. (2010). Young Children's Play in Online Virtual Worlds. *Journal of Early Childhood Research, 8(1),* 23–39, https://doi.org/10.1177/1476718X09345406

Nhan, J. & Bowen, K. N. (2020). Policing Internet Sex Trafficking. *Journal of Qualitative Criminal Justice and Criminology, 9(1),* https://doi.org/10.21428/88de04a1.2d5eb46e

Quayle, E. (2020). Prevention, Disruption and Deterrence of Online Child Sexual Exploitation and Abuse. *ERA Forum 21,* 429–447. https://doi.org/10.1007/s12027-020-00625-7

Raposo, V. L. (2023). The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal. *European Journal on Criminal Policy and Research, 29,* 515–533, https://doi.org/10.1007/s10610-022-09512-y

Roche, S., Otarra, C., Fell, I., Torres, C. B. & Rees, S. (2023). Online Sexual Exploitation of Children in the Philippines: A Scoping Review. *Children and Youth Services Review, 148.* https://doi.org/10.1016/j.childyouth.2023.10686

Rustad, M. B., Parsanoglou, D., Symeonaki, M., Mifsud, L., Hyggen, C. & Ghetau, C. (2024). Of Gaming and Other Demons: Defining Children and Young People's Meaningful Leisure Activities in the Digital Era. In:

H. Holmarsdottir, I. Seland, C. Hyggen, & M. Roth (Eds.), *Understanding The Everyday Digital Lives of Children and Young People, Palgrave Macmillan,* 281–320.

Sirola, A., Savela, N., Savolainen, I. *et al*. (2021). The Role of Virtual Communities in Gambling and Gaming Behaviors: A Systematic Review. *Journal of Gambling Studies, 37,* 165–187. https://doi.org/10.1007/s10899-020-09946-1

Stasi, M. L. (2019). Social Media Platforms and Content Exposure: How to Restore User's Control. *Competition and Regulation in Network Industries, 20(1),* 86–110, https://doi.org/10.1177/1783591719847545

Victoria Baines. (2019). Online Child Sexual Exploitation: Towards An Optimal International Response. *Journal of Cyber Policy, 4(2),* 197–215, https://doi.org/10.1080/23738871.2019.1635178

Witting, S. K. (2021). Transnational by Default: Online Child Sexual Abuse Respects No Borders. *The International Journal of Children's Rights, 29(3),* 731–764. https://doi.org/10.1163/15718182-29030010

Woodhams, J., Kloess, J. A., Jose, B., Hamilton-Giachritsis, C. E. (2021). Characteristics and Behaviors of Anonymous Users of Dark Web Platforms Suspected of Child Sexual Offenses. *Frontiers in Psychology, 12,* https://doi.org/10.3389/fpsyg.2021.623668

Other sources

BBC News. *Prolific Pedophile Mark Frost Admits to Abuse in UK and Asia*. [Online] (modified 2017-02-01). Available at: https://www.bbc.com/news/uk-38830191 [Accessed 27 March 2024].

Muhammad Imran Ali LL.M. areas of scientific interest are Constitutional Law, International Law, Criminal Law and Child Rights.

Muhammado Imrano Ali, LL.M. mokslinių interesų sritys yra konstitucinė teisė, tarptautinė teisė, baudžiamoji teisė ir vaiko teisės.