JOURNAL OF MULTIDISCIPLINARY ISSUES
Journal Website: www.jmis.site
J. Multidisc. Issues 3(1) 13 - 29 (2023)

CHILD/REVENGE PORNOGRAPHY IN THE REPUBLIC OF MAURITIUS: EXTENT, CHALLENGES, AND POTENTIAL APPROACHES FOR PREVENTION, DETERRENCE, AND MITIGATION

Viraj Fulena[a], Hemant B. Chittoo[b]
[ab] University of Technology, Mauritius
[*] vfulena@utm.ac.mu

ABSTRACT *The phenomenon of Child/Revenge Pornography in the Republic of Mauritius is a sensitive and controversial one. Many may prefer to keep it as a taboo subject. The figures of the extent of the phenomenon are, however, appalling. The most recent figures available from official sources show 1,835,064 attempts in the period 2011 to 2021 to access Child Sexual Abuse sites and 110,026 Mauritian IP addresses having to do with Child Sexual Abuse that have been blocked by ICTA in the same 10-year period. It will not be exaggerated to infer that the situation of 'moeurs' in the Republic of Mauritius is deteriorating.*
Objective – *The Government of Mauritius has been reasonably proactive and kept with its tradition of honouring its international obligations all by enacting appropriate laws, like the Children's Act 2020 and the Cybersecurity and Cybercrime Act 2021 to ensure the problem does not spill out of control. These laws provide a legal framework for addressing various forms of child exploitation and cybercrimes, including child and revenge pornography. They empower law enforcement agencies to investigate and prosecute those involved in these activities. However, the phenomenon is one whereby any single new case is a case 'de trop' for the self-respect of a society, for the image and health of society, for the psychological security of victims and has the risk of giving give rise to public outcries. Stricter laws to deter and punish perpetrators, while always welcome, do not reflect a healthily educated and mature society, ethically compliant in terms of desirable behaviour of the great majority of its citizens.*
Methodology – *In order to ensure the robustness of findings and recommendations that emerge, An assessment of the situation based on the review has been done through a semi-structured questionnaire, one to one interview, and a consultative workshop with stakeholders.*
Findings – *This paper has revealed the realistic hard and soft, short, medium and long-term solutions to attack the problem at its root cause.*
Novelty – *Wide consultation via literature review, one-to-one interviews, focus groups of stakeholders and member of Government and Non-Government Organizations, the media, academics, and opinion leaders, among others, do reveal a common understanding of the phenomenon, its extent, its root causes, the legal and institutional framework to combat the phenomenon, their adequacy and effectiveness, and further solutions that can be envisaged for a better Mauritius for our present and future generations.*
Keywords: *pornography; assesment; semi-structured questionnaire; child sexual abuse*

JEL Classification: I00, I39, Z00
Article Info: *Received 05 August 2023, Revised 10 Dec 2023, Accepted 18 Dec 2023*
Article Correspondence: vfulena@utm.ac.mu
Recommended Citation: Fulena and Chittoo (2023). *Child/Revenge Pornography in the Republic of Mauritius: Extent, Challenges, and Potential Approaches for Prevention, Deterrence, and Mitigation*. Journal of Multidisciplinary Issues, Issues 3(1) 13-29

I. INTRODUCTION

There is wide consensus that Child revenge pornography involves the sharing of sexual, images or videos, **without the consent** of the child in the image. It is noteworthy that there is some confusion as to where to

draw the line between pornography and revenge pornography. The key in the difference lies in the 'no consent'.

In the same line, there are concerns to the effect that the concept of child, although making the crime of revenge pornography more heinous, should not deter similar crimes committed on adults. The focus should rather be on 'Revenge Pornography'.

Revenge pornography can be defined as the distribution or dissemination of sexually explicit images or videos of individuals without their consent. The sexually explicit images or video may be made by a partner in an intimate relationship with the knowledge and consent of the subject at the time, or it may be made without their knowledge.

- First element to be satisfied is the non-consensual distribution or dissemination of sexually explicit images.
- The second element is the intention behind such distribution or dissemination of images.
- The motive of perpetrators of revenge porn may be to coerce victims into continuing a relationship or to punish them for ending the relationship (in case of relationship), to silence them, to destroy their reputation, and/or for financial gain. Coercive control is often the aim behind revenge pornography.
- The intent of "revenge pornography" is to humiliate and intimidate the subject by uploading and distributing sexually explicit images or videos featuring the subject or subjects.
- The intention behind diffusing such images is distinctive. Non-consensual pornography may not always be revenge pornography. It is the intent element which qualifies it as revenge pornography.
- The perpetrator must "act maliciously" to jeopardise the victim and his/her future relationship. It will involve a breach of trust by perpetrators who usually target the sexual integrity and damaging the identity of the victims.
- The practice has also been described as a form of psychological, sexual abuse.
- It is an issue amongst all ages, from children of young age to older adults.

Research Questions:

1. What is the extent of child and revenge pornography in the Republic of Mauritius, and how has it evolved over time?
2. What are the root causes of child and revenge pornography in Mauritius, and what are the contributing factors to its persistence?
3. How effective have the existing legal and institutional frameworks, including the Children's Act 2020 and the Cybersecurity and Cybercrime Act 2021, been in addressing child and revenge pornography in Mauritius?
4. What are the short-term, medium-term, and long-term solutions to combat child and revenge pornography in Mauritius at its root cause?
5. What are the key priority areas for action and recommendations for a safer online environment for children and adults in Mauritius?

Research Objectives:

1. To assess the prevalence and trends of child and revenge pornography in Mauritius over the past decade, using available data and statistics.
2. To identify the underlying causes and factors contributing to the proliferation of child and revenge pornography in the Mauritian context.
3. To evaluate the effectiveness of the legal and institutional frameworks, including the Children's Act 2020 and the Cybersecurity and Cybercrime Act 2021, in addressing child and revenge pornography, considering their strengths and weaknesses.
4. To propose evidence-based solutions for addressing child and revenge pornography in Mauritius, including short-term interventions, medium-term strategies, and long-term preventive measures.
5. To generate actionable recommendations for policymakers, law enforcement agencies, NGOs, and other stakeholders to create a safer online environment and protect individuals of all ages from the harm caused by child and revenge pornography.

II. LITERATURE REVIEW

Consensual vs. Non-Consensual Pornography:

There exists a clear demarcation between consensual and non-consensual pornography. In consensual adult pornography, all parties involved are of legal age, and the participants willingly provide their consent for the creation and distribution of explicit content. The key differentiator between consensual and non-consensual pornography is the issue of consent (Wolak, Mitchell, & Finkelhor, 2007). It's important to emphasize that, in consensual pornography, individuals are legally able to provide consent, whereas in non-consensual cases, consent is absent, and often coercion or malicious intent is involved (Krieger, Tymula, Glimcher, Levy, & Louie, 2017).

Protecting individuals exposed to non-consensual pornography, particularly minors, is of paramount concern. Safeguards are necessary to provide legal recourse and support for these victims. Many countries, including Mauritius, have introduced laws specifically targeting non-consensual pornography. These laws empower victims to take legal action against perpetrators (Citron & Franks, 2014). Providing accessible and confidential reporting mechanisms is essential for minors who have been exposed to non-consensual pornography. These mechanisms allow victims to seek assistance and initiate investigations (Citron, 2014).

It's crucial to have support services in place, including counseling and legal aid, to help victims cope with the emotional and psychological effects of non-consensual pornography (Döring, Daneback, & Shaughnessy, 2017). Educational programs and awareness campaigns can help educate minors about the risks associated with explicit content and the importance of reporting any form of abuse (Albury, Crawford, & Byron, 2013).

Non-consensual pornography can have severe and long-lasting effects on minors. It can lead to emotional distress, trauma, and a range of negative consequences, including social isolation and bullying (Mitchell, Wolak, & Finkelhor, 2007). Ensuring safeguards are in place is critical to protecting the well-being of young victims.

By exploring the differences between consensual and non-consensual pornography and discussing the safeguards in place to protect minors exposed to non-consensual explicit content, this review highlights the need for comprehensive legal and support systems to address these issues effectively.

Government Initiatives in Mauritius:

As mentioned above, the Government of Mauritius has taken legislative steps to address the issue. As mentioned earlier, the government enacted the Children's Act in 2020 and the Cybersecurity and Cybercrime Act in 2021. These laws provide a legal framework for addressing various forms of child exploitation and cybercrimes, including child and revenge pornography. They empower law enforcement agencies to investigate and prosecute those involved in these activities. Promoting awareness and education is a critical component of addressing these issues. The government, in collaboration with various stakeholders, has initiated awareness campaigns and educational programs aimed at informing the public, especially young people, about the risks associated with sharing explicit content online and how to protect themselves. Mauritius has been working with international organizations and agencies, such as INTERPOL and UNICEF, to combat child exploitation, including child and revenge pornography. Collaboration on information sharing, best practices, and training for law enforcement agencies is essential to tackle these issues effectively. Moreover, the government has established specialised cybercrime units within its law enforcement agencies to investigate and combat online crimes, including child and revenge pornography. These units are equipped with the necessary skills and technology to address digital threats. Setting up hotlines and reporting mechanisms for the public to report instances of child or revenge pornography is crucial. These channels allow individuals to report incidents anonymously, and law enforcement agencies can then take appropriate action.

It is important to keep in mind that addressing child and revenge pornography is an ongoing process that requires continuous adaptation to the changing digital landscape. Providing support services for victims of child and revenge pornography is essential. The government, in conjunction with NGOs and support organizations, offers counselling and legal assistance to victims to help them cope with the emotional and legal aspects of their situations. Mauritius has always kept a very good diplomatic relationship with its

counterparts and has been party to international agreements and conventions related to child protection, such as the United Nations Convention on the Rights of the Child. These agreements guide the government's efforts to protect children and address child exploitation issues.

According to a report from INTERPOL, there has been a significant increase in the distribution of child sexual abuse material (CSAM) over the internet in the last decade. In 2020, there were over 22 million reports of CSAM, and a considerable portion of this material involved children from various countries, including Mauritius. Based on a report issued by the International Centre for Missing & Exploited Children (ICMEC), approximately 1 in 7 children globally received unwanted sexual solicitations online. Furthermore, the proliferation of digital technology has contributed to the rise of such incidents, with an increase in cases of non-consensual distribution of intimate images and videos.

During a collaborative workshop organized by the Ministry of Gender Equality and Family Welfare and the University of Technology, Minister Koonjoo-Shah emphasized the prevalence of global online child sexual abuse and exploitation. The event, which took place at the Ravenala Attitude Hotel in Balaclava, Mauritius in 2020, aimed to establish effective Standard Operating Procedures, identify legislative gaps, promote research analysis, and provide actionable recommendations concerning child and revenge pornography in Mauritius (Ministry of Gender Equality and Family Welfare and University of Technology, 2020).

Drawing attention to the India Child Protection Fund, Minister Koonjoo-Shah highlighted the staggering increase in the usage of pornography websites by 95% during the 2020 lockdown period. Additionally, she pointed out that website monitoring data revealed a notable spike in search terms such as 'child porn,' 'sexy child,' and 'teen sex videos' during the same period (Ministry of Gender Equality and Family Welfare and University of Technology, 2020).

The Minister emphasized that the rising use of technology and the internet had contributed significantly to this societal issue, affecting Mauritius as well. She cited recent instances of child/revenge pornography, in which telecommunication and social media platforms like Telegram and Facebook were exploited to disseminate explicit photographs of children and videos of women and girls (Ministry of Gender Equality and Family Welfare and University of Technology, 2020).

III. METHODOLOGY

In order to ensure the robustness of findings and recommendations that emerge, a rigorous set of methods has been used as detailed below:

a. A desk review scoping the child and revenge pornography situation in the Republic of Mauritius was carried out. This included identifying and reviewing existing literature on online child sexual exploitation. Literature included peer reviewed articles, and gray literature such newspaper articles, NGO reports, and conference reports. It also included identifying key actors.
b. Based on the desk review and initial conversations with the team management, the methodology was refined for conducting a review of the situation in Mauritius;
c. An assessment of the situation based on the review has been done through a semi-structured questionnaire, one to one interview, and a consultative workshop with stakeholders.

IV. RESULTS AND DISCUSSION

A. LEGAL FRAMEWORK IN MAURITIUS

Attention should be drawn to the fact that understanding of the definition and applicable legal framework of many, if not some stakeholders, were not up to date. This is a clear indication that efforts will be required to sensitize, educate and train many segments of stakeholders about the proactive measures that government has already taken to re-actualize existing pieces of legislations and the introduction of new legal and institutional frameworks to better tackle the phenomenon in the Republic of Mauritius.

The Children's Act 2020 (assented on 18 Dec 2020) which is a more comprehensive legislation than the repealed Child Protection Act 1994, deals with Child Pornography in its Section 21. It is therein stated that no person shall -

(a) knowingly obtain access, through information and communication technologies, to child pornography;
(b) produce, possess, procure, obtain, import, export or distribute child pornography, whether or not through information and communication technologies, for himself or for another person;
(c) view, supply, disseminate, offer or make available child pornography and any other pornographic material; or
(d) coerce, force or otherwise induce a child to view a pornographic performance or pornographic material, or to witness a sexual act

Child Pornography also includes under section 21 –
(a) any representation by whatever means where a child is or appears to be engaged in real or simulated explicit sexual activities; or
(b) of the sexual parts of a child, primarily for sexual purposes.

It is to be noted that any person who commits an offence under section 21 shall on conviction be liable to a term of imprisonment not exceeding 20 years where the child is physically or mentally handicapped. In other cases, it is not exceeding 10 years.

The **Cybersecurity and Cybercrime Act 2021** defines pornography as the representation in a book, magazine, photograph, film, computer data or any such other media or a scene of sexual behaviour in any form that is erotic or lewd and is designed to arouse sexual interest. It further defines revenge pornography specifically in its section 19. It is provided that any person who, by means of a computer system, discloses or publishes a sexual photograph or film without the consent of the person who appears in the photograph or film, and with intention of causing that person distress, shall commit an offence and shall, on conviction, be liable to a fine not exceeding Rs. 1 million and to penal servitude for a term not exceeding 20 years. It is to be noted that, under the said Act, computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

B. EXTENT/SPREAD OF CHILD PORNOGRAPHY IN MAURITIUS (INCLUDING RODRIGUES)

The extent/spread of the phenomenon is difficult to ascertain as there have been but few cases of reported offences and same have been referred to relevant units of the Police Department dealing with IT and cyber security. It could also be ascertained that it may be difficult to reconcile figures from different institutions, possibly because of different objectives of collecting data and differentials in concepts and terminologies used. A reliable source of data/information would be the ICTA with respect to number of hits on CSA sites and the Mauritius Police Force would be reliable with respect to statistics of reported offences.

The Online Content Filtering (OCF) solution implemented by ICTA has allowed the filtering of 1,835,064 attempts (hits) to access CSA websites by Mauritian users and the blocking of 110,026 Mauritian IPs addresses since the implementation of the system in 20111. Tables 1 and 2, and Figures 1 and 2 in this report give a good indication of the extent of the phenomenon. The figures keep on rising and currently different organizations are keeping statistics for their own use

[1] "Note by the Information and Communication Technologies Authority (ICTA). Child Sexual Abuse (CSA° Filtering Mechanism updates on Child protection Initiative – ITU", Document CWG-COP-18/5-E, ITU Council Working Group on Child Online Protection, 18th meeting – Virtual, 12 January 2022.

and what they would find useful from their perspectives, as for instance, can be depicted in table 3 below.

Cybercrime Incidents Reported to CERT-MU from 2020 to 30 April 2022

Note: The incidents in table 1 are cases reported to CERT-MU through the online Platform MAUCORS (Mauritian Cybercrime Online Reporting System). Selected data have been extracted on incident types which occur mainly on the social media platforms where incidents reported involve youngsters. The platform does not specifically categorize child related incidents in its system.

Table 1 Cybercrime Incidents Reported to CERT-MU from 2020 to 30 April 2022

Incident Type	**Number Reported**
Hacking	1122
Online Harassment	1267
Offensive Content	714
Sextortion	219
Identity Theft	634
Cyber Bullying	313
Cyber Stalking	70
Total	**4339**

Source: MAUCORS (May 2022)

The desire to buy local products, particularly local foods, can contribute to long-term food sustainability. The problem is that individuals are uninformed and unaware of the necessity of food sustainability, which leads them to choose to throw away food, resulting in food shortages or scarcity. Furthermore, with the rising diversity of food ingredients, each location or nation has its own commodities advantages, the public is paying less attention to the local foods sector, which really delivers many benefits to local producers as well as the country itself. Local foods have their own benefits, including the fact that they are more nutritious because they are not further processed, that they can help reduce greenhouse gas emissions in the atmosphere, and that they can open up employment opportunities, particularly in the tourism sector, to promote healthy diets that will ultimately be in the hands of consumers themselves. As a result, collaboration between

the government and the public is required to raise awareness of the necessity of preserving food sustainability, particularly in local foods, in the face of changing lifestyles and external pressures that have reduced public awareness. Food sustainability cannot be reached in a short period of time; nevertheless, with a long-term perspective, the outcomes acquired will be equivalent to or even better than present goods.

C. EXAMPLES OF CASES AND LESSONS LEARNT FROM FOCUS GROUPS AND CASE LAW

Based on responses of stakeholders and lessons learnt from youth programmes and interaction with young people, and in an attempt to maintain anonymity and ethical reporting, the following can be summarized as being of relevance and informative:

(i) The scandal on telegram where more than 1200 pictures of women and children were shared, was like a blow in our society. Enquiry was instituted by the Cyber Crime Unit.

Lessons Learnt: Social Media allows sharing of pornographic material as any other material like wild fire. The extent of damage to victims are inestimable and, in all likeliness, irreparable.

(ii) There exists a reported case in 2014 when two young adolescents filmed their sexual relationship and finally the young boy, aged 17 shared the films to attempt to ruin the life of the young girl after they broke their relationship.

Lessons learnt: The two young persons were warned by police at the request of DPP. No action has been taken against the persons who shared the films. Taking appropriate action is a deterrent to preventing sharing of pornographic materials. The two young persons involved had to leave their place of residence so that people can forget about them. This was considered as a good move as the young girl had the opportunity to continue to study and is now in employment.

(iii) Another case where an employee of a college took pictures of young students when they were in the changing room. The latter used the photos for his pleasure and it came to light after his daughter discovered 101 films and reported the case to the police which found photos of young students on his laptop

Lessons learnt: Action has been taken against the Employee. He was dismissed from the College. Some of the young women identified in the films refused to report a case against the Employee as they were on their way to University. Others refused as reporting a case against the perpetrator would put to light their intimacy. Such cases take too much time before prosecution, in the meantime, the youngsters preferred to do something else than wait for the prosecution and they would have to attend Court several times.

(iv) Another known case is the “pedo-pornographic case” reported in 2021. More than 2000 sexual images and films of young persons, were found on a mobile phone belonging to a young man. The latter came to know many of those people he filmed as a result of a privileged position he held. Unfortunately, not all the victims came forward to report cases against him. The films are in the possession of police (CID) and are still under investigation.

Lessons Learnt: There has been too much publicity for this case. This refrained victims from coming forward to report the case. It is suspected that the young man may have gathered much

information on his victims while being in his position. This young man was known to organize "sexual" parties when he was young. Unfortunately, he has never been caught and as such, no case has been reported against him. His clean certificate of character permitted him to find a job. The case also puts in perspective the importance of ethical and responsible reporting by the media so as not to make victims ashamed to come forward against perpetrators.

Generic Lessons learnt:

- duty-bearers have not been able to protect children from this illegal malpractice;
- existing laws did not deter perpetrators in targeting children and dragging them in pornography;
- public, parents and legal guardians are not aware about the magnitude of such a problem existing in our society or do not pay much attention to it to protect their children or young citizens;
- there might be a need for more focused sensitisation programmes in pre-primary, primary and secondary schools, tertiary institutions, involving parents, caretakers and teachers to detect any such cases (from the behaviour of children);
- There must be a concerted approach amongst relevant stakeholders when dealing with such cases (e.g. Cyber Crime Unit; ICTA; CERT.MU, Police, Ministry of Gender Equality and Family Welfare, Ombudsperson for Children, Media);
- The cases brought forth the need to have more sensitization campaigns on the issue of child revenge pornography to create awareness among the minors as well as adults, especially parents and teachers so that they fully understand the extent of harm that such a practice can generate. The best interest of children and their holistic development can be much affected by such practice;
- If prevention programmes are not undertaken to instill appropriate measure of fear in minors in terms of legal implications [Fines and imprisonments have been clearly stipulated in the Children's Act 2020, and Cybersecurity and Cybercrime Act 2021 as regards issues related to child/revenge pornography], they may think that such practices are normal and continue same with even worse outcomes.

D. CURRENT MEASURES IN THE INSTITUTIONAL FRAMEWORK TO:

- **Deter**
- **Prevent**
- **Punish perpetrators**
- **Protect victims**

Mauritius is signatory to international treaties, for example, Human Rights Convention which include the right of children, whereby, protection of children from all/any kind of harm have been mentioned. The judicial system of Mauritius and concerned stakeholders have to abide and uphold those treaties. There are mechanisms to prevent likelihood of such malpractices.

Deterrence Measures

Information and Communication Technologies Act 2001

This Act has been implemented to regulate and democratise ICT and related matters. The Act makes it an offence for people making wrongful use of information and communication service. Offences such as Cyber Bullying can be prosecuted under this Act.

Ensuring a safe digital environment for Mauritian children is of utmost concern to the regulatory Authority of Mauritius2. Since 2011, the ICTA has implemented a Child Sexual Abuse Material (CSAM) filtering mechanism, in line with the ITU guidelines on Child Online Protection3.

Even though the protection of children online is a relatively recent area of public policy concern4, ICTA has been proactive as a regulator in addressing the issue ever since 2011. This is in line with the fact that regulatory agencies are at the forefront of worldwide public policies for children's protection online5.

Two major approaches are usually adopted by regulators over the world to curb CSAM: notice and take down procedures (mandatory in Australia, Italy, Japan, Korea and Turkey) and/or filtering schemes (Turkey, Australia) 6. The latter option has been adopted by the Information and Communication Technologies Authority (ICTA) of Mauritius to fight and prevent child sexual abuse online7.

The mandate of ICTA regarding Child Sexual Abuse Material8

Pursuant to Sections 18(1)(m) and (n) of the ICT Act 2001, as amended, the Authority is empowered to *"take steps to regulate or curtail harmful and illegal content on Internet and other information and communication services" and "ensure the safety and quality of any information and communication services".* This provision of the ICT Act 2001 is also congruent with Section 251 "Debauching youth" of the Criminal Code Act, section 86 of the Criminal Code (Supplementary Act) which makes it an offence for any person to deal with obscene matters,

[2] "Note by the Information and Communication Technologies Authority (ICTA). Child Sexual Abuse (CSA° Filtering Mechanism updates on Child protection Initiative – ITU", Document CWG-COP-18/5-E, ITU Council Working Group on Child Online Protection, 18th meeting – Virtual, 12 January 2022.

[3] Child Sexual Abuse Material (CSAM) refers to "*any material that visually depicts a child in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes*". This includes photography, video, drawings, cartoons, text and live streaming. International Telecommunication Union (ITU) and United Nations Children's Fund (UNICEF), "Guidelines for Industry on Child Online Protection", 2015.

[4] OECD (2011-05-02), "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", *OECD Digital Economy Papers*, No. 179, OECD Publishing, Paris, p. 32. [http://dx.doi.org/10.1787/5kgcjf71pl28-en]

[5] Ibid., p. 33.

[6] Ibid., p. 33.

[7] "Note by the Information and Communication Technologies Authority (ICTA). Child Sexual Abuse (CSA° Filtering Mechanism updates on Child protection Initiative – ITU", Document CWG-COP-18/5-E, ITU Council Working Group on Child Online Protection, 18th meeting – Virtual, 12 January 2022.

[8] "Note by the Information and Communication Technologies Authority (ICTA). Child Sexual Abuse (CSA° Filtering Mechanism updates on Child protection Initiative – ITU", Document CWG-COP-18/5-E, ITU Council Working Group on Child Online Protection, 18th meeting – Virtual, 12 January 2022.

Section 21 "Pornography" of the Children's Act 2020 and the Cybersecurity and Cybercrime Act 2021 which criminalize sexual offences perpetrated on children (as detailed earlier in the report).

The ICTA's project on CSAM filtering is also pursuant to the recommendations of the UN Committee on the Rights of the Child. In its 2014 report on "*Digital media and children's rights*", the UN Committee on the Rights of the Child has called on regulatory agencies to demonstrate responsibility in developing standards relevant to children's rights and ICTs. In its endeavour, the ICTA is opening up a pathway for best practices, relying on international cooperation to support the process9.

As acknowledged by *ITU Guidelines for policy makers on COP* (2020), empowering the regulatory authority to intercede with such contents provides an important safeguard for children rights and safety in a number of ways:

- By providing a rapid response, of crucial importance in such situations;
- By providing path-breaking practices for addressing the issue of CSAM that can pave the way for further legal reinforcement10;
- By allowing the reinforcement or development of good standards, as underlined in the 2021 ITU policy brief11.

With this in view, in order to fulfil its mandate, the ICTA has implemented a Centralized Online Content Filtering (OCF) solution.

The Children's Act 2020 in Section 21 and the Cybersecurity and Cybercrime Act 2021 make provision for higher penalties for Child pornography as follows -

The Children's Act 2020

(1) No person shall –

(a) knowingly obtain access, through information and communication technologies, to child pornography;

(b) produce, possess, procure, obtain, import, export or distribute child pornography, whether or not through information and communication technologies, for himself or for another person;

(c) view, supply, disseminate, offer or make available child pornography and any other pornographic material; or

(d) coerce, force or otherwise induce a child to view a pornographic performance or pornographic material, or to witness a sexual act.

(2) Any person who commits an offence under subsection (1) shall, on conviction, be liable –

9 "Note by the Information and Communication Technologies Authority (ICTA). Child Sexual Abuse (CSA° Filtering Mechanism updates on Child protection Initiative – ITU", Document CWG-COP-18/5-E, ITU Council Working Group on Child Online Protection, 18th meeting – Virtual, 12 January 2022.

10 ITU, *Guidelines for policy-makers on Child Online Protection 2020*, pp. 32-33.

11 ITU, Policy brief "Keeping children safe in the digital environment: The importance of protection and empowerment", October 2021, p.6.

(a) where the child is physically or mentally handicapped, to penal servitude for a term not exceeding 20 years;

(b) in any other case, to penal servitude for a term not exceeding 10 years.

Institution of a Children's Court

The Children's Court Act 2020 has made provision for Children's Court which is already in operation. With respect to *Testimony of witnesses*: As per section 161A of the Courts Act, it is possible to make a motion for a child witness to be heard *in camera.* This means that the public is excluded from the court during the testimony of the child. Only the court staff, the accused and the legal representatives remain in court. Section 161A may also be used for adult witnesses in sexual offences. The magistrates of the Children's Court could be motivated to protect victims by leveraging such provisions of the legal framework in Mauritius.

Cybersecurity and Cybercrime Act (2021)

Section 19-Revenge pornography from the Cybersecurity and Cybercrime Act (2021) refers. The section is clear to the extent that "any person who, by means of a computer system, discloses or publishes a sexual photograph or film without the consent of the person who appears in the photograph or film, and with the intention of causing that person distress, shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to penal servitude for a term not exceeding 20 years."

Data Protection Act 2017

The Mauritius Data Protection Act, 2017 (DPA) governs privacy rights of individuals in relation to requirements of collection, processing, storage, transfer and handling of personal information/sensitive personal information. It remains one of the laws under which prosecution of perpetrators can be envisaged.

Prevention Measures

Some preventive measures/initiatives that are in force in the present institutional framework are as detailed below:

Initiatives by CERT-MU to promote safe usage of the Internet among youngsters

1. Organisation of the Safer Internet Day

The Safer Internet Day is an international event and its main objective is to promote safe and responsible use of the Internet and mobile devices amongst youngsters. CERT-MU is responsible to organise this event in Mauritius to promote the safe usage of the Internet among youngsters. Various activities are carried out for students, teachers and parents to empower them on Online Safety. The theme for this year's SID is "Together for a Better Internet". The following activities were organized by CERT-MU in February 2022:

a. Production of video clips on Internet safety;

b. A digital guideline on best Internet practices for youngsters;

c. Dissemination of Safety tips on a weekly basis to all public officers;

d. Online awareness sessions for youngsters, students & teachers; and

e. Organization of an online webinar for University students in collaboration with Federation of Innovative & Numeric Activities in **Mauritius** (FINAM).

2. Organization of Sensitization Campaigns in schools

Based on the requests made by schools and colleges, CERT-MU carries out presentations and talks for students from different schools and colleges throughout the whole year across the island of Mauritius.

3. Awareness Campaigns through the Media

CERT-MU participates in MBC Radio Programmes regularly to promote the safe usage of the Internet. The Ministry of Gender Equality and Family Welfare has also been participating on such platforms.

4. Sensitization through Community Centers

CERT-MU carries out presentations on the dangers of Internet mainly for housewives through Village Community Centers. The activities being carried out by CERT-MU are useful and should be pursued in the future.

Initiatives by the Mauritius Police Force

Sensitisation campaigns and awareness by the different Units of the Mauritius Police Force are also being organized and items like cyber bullying, child pornography, online offences should be included in the programmes if not already the case. Awareness campaigns are held in educational institutions with the collaboration of Ministry of Education; Youth and Community Centres in concertation with the SILWF and ministries concerned. These initiatives should be continued with more rigour and frequency. Cyber patrols are done on a daily basis by the Cyber Crime Unit of the Central Criminal Investigation Division (CCID). The CCID works closely with the Interpol.

Punishment of Perpetrators

The advent of the Cybersecurity and Cybercrime Act 2021; Children's Act 2020, Combatting of Trafficking in Persons Act 2009, will enable Law Enforcement Officials to enforce these laws and bring offenders to the criminal justice system.

The penalty under the Cybersecurity and Cybercrime Act 2021 is heavier and will act as a strong deterrent factor in the society.

Protection of Victims

A special desk with dedicated team from the Cyber Crime Unit and the Brigade Pour La Protection de La Famille (BPF -formerly known as PFPU) deal with such cases.

Victims are given psychological follow-ups by professionals from the Ministry of Gender Equality and Family Welfare. Moreover, the Child Development Unit (CDU) works directly with children

undergoing any kind of neglect, abuse or violence. CDU has the authority to remove child at risk even from biological families/caretakers and place them in Shelters for immediate follow-ups.

The National Youth Policy (NYP) 2016 recognises the fundamental rights and liberties guaranteed by the Constitution of the Republic of Mauritius which has signed and ratified several international conventions on the rights and welfare of the child.

The NYP lays emphasis on the recognition on the rights of youth to life and security, love and affection, privacy and protection from all forms of abuse, neglect and exploitation including harassment, violence and cruel treatment. It also refers to the right to access to information, education and training and a healthy environment (NPY 2016, pg. 9). The policy also lays emphasis on the responsibilities of parents/responsible parties to ensure provision of an environment of affection, security and psychological development (pg. 11). Clearly there are indications for further sensitization and training of the Youth by the authorities.

E. FUTURE MEASURES TO ALLEVIATE THE PROBLEM

- **in the short term**
- **in the medium term**
- **in the long term**

AT LEVEL OF THE ICTA

In order to fight and prevent Child Sexual Abuse (CSA) online, the Information and Communication Technologies Authority (ICTA) has adopted a filtering solution, based on international partnership and using the method of blacklisting. Thanks to the collaboration with UK-based NGO, Internet Watch Foundation (IWF) since 2013, ICTA has implemented a filtering mechanism to prevent Internet users in Mauritius to access to CSA material.

This Online Content Filtering (OCF) solution implemented by ICTA has allowed the filtering of 1,835,064 attempts (hits) to access CSA websites by Mauritian users and the blocking of 110,026 Mauritian IPs addresses since the implementation of the system in 2011 to 202112. This OCF solution has been presented by the ICTA in an official presentation to the ITU COP Initiative, extracts of which are presented below.

<u>The Child Sexual Abuse (CSA) Filtering Mechanism: Scope and Purpose</u>

The CSA filtering is the flagship of the ICT Authority's intervention and participation in the prevention of pedo-pornography and CSA online. It was launched in February 2011 and further reinforced through a cooperation agreement with the UK-based NGO Internet Watch Foundation (IWF) as from 2013. The OCF solution filters access to Child Sexual Abuse (CSA) sites for Internet users in the Republic of Mauritius. The objective was two-fold13:

[12] "Note by the Information and Communication Technologies Authority (ICTA). Child Sexual Abuse (CSA° Filtering Mechanism updates on Child protection Initiative – ITU", Document CWG-COP-18/5-E, ITU Council Working Group on Child Online Protection, 18th meeting – Virtual, 12 January 2022.

[13] "Note by the Information and Communication Technologies Authority (ICTA). Child Sexual Abuse (CSA° Filtering Mechanism updates on Child protection Initiative – ITU", Document CWG-COP-18/5-E, ITU Council Working Group on Child Online Protection, 18th meeting – Virtual, 12 January 2022.

- Reduce the availability and circulation of CSA material in Mauritius, hence limiting the trauma experienced by the victims and their families; and

- Offer greater protection against accidental viewing.

The filtering solution for CSAM prevention opted for by ICTA is based on the method of blacklisting14. It involves the use of the Internet Watch Foundation (IWF) database, which backlists such websites or web pages. THE OCF solution actually contains two aspects: (a) reporting through IWF portal and (b) the filtering system through the NetClean Whitebox technology.

a) The reporting system through IWF portal

A Memorandum of Understanding (MoU) was signed between IWF and ICTA on 24 October 2013 for a duration of two years. Its objective was to enable Internet users in the Republic of Mauritius to report suspected illegal CSAM hosted anywhere in the world via the dedicated platform of IWF, namely the Online Child Sexual Abuse Reporting Portal (OCSARP) 15. Reporting details of CSAM via the OCSARP portal allows:

(1) assessment against the legality according to UK or Mauritian law,

(2) identification of the actual location of the material, and

(3) undertaking appropriate actions to have the material removed at the source by IWF.

The mechanism comprises the linking of the IWF blacklist with local Internet Service Providers in the Republic of Mauritius via the ICTA website. Under this MoU (2013-2015), the IWF worked in partnership with ICTA to provide a reporting portal available via the ICTA website (www.icta.mu) for individuals or organisations to report potential CSAM. It assessed the online material and assisted the service providers to avoid abuse of their systems by distributors of CSAM.

Regarding potentially illegal content hosted in the UK and/or the Republic of Mauritius, the IWF collaborated with the competent authorities to have the contents taken down and the offender detected. In case where the potentially illegal content was hosted outside the UK or the Republic of Mauritius, the IWF worked in partnership with hotlines across the world and various enforcement bodies both in the UK and abroad to have the content investigated. Even if some of the material remains available online, it is included on the IWF blacklist and blocked to stop inadvertent exposure. The IWF blacklist is updated on a daily basis.

14 Filtering can be based on two different methods: blacklist or whitelist. Whitelists block access to all web contents except when listed as suitable for the user, whereas blacklists enable access to all web contents except when listed as inappropriate for the user. OECD, "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", op. cit., p. 65.

15 Memorandum of Understanding between IWF and ICTA, 24 October 2013.

The reporting system via the OCSARP portal was operational until the expiry of the MoU in October 201516. However, even after the expiry of the MoU, ICTA kept using the IWF blacklist for its filtering system.

b) The filtering system: the NetClean Whitebox technology

Filters can be deployed at various levels of the ICT infrastructure: at network level, server level or end-user terminal level. The most efficient one being the filtering at network level17, which is the solution that has been retained by ICTA18.

The ICTA has been blocking access to CSAM for viewing in Mauritius through the CSA filtering system which is linked with all local Internet Service Providers licensed by the ICT Authority.

The CSAM filtering mechanism set up by the ICTA makes use of the IWF database, which is updated daily and blacklists the CSAM websites or pages, preventing them from being accessed by Internet users in the Republic of Mauritius.

The centralised filtering system serves as a cybersecurity infrastructure shared among ISPs and managed by the ICTA. Once IWF adds any website or web page to its black list, the ICTA's filtering system is automatically updated so that the newly added websites or web pages can no longer be accessed to from Mauritius. Therefore, even when the removal of the offensive content cannot be performed at the source19, the filtering system ensures that it can no longer be viewed from Mauritius.

To implement this centralised filtering solution, the ICTA has been using the NetClean Whitebox technology developed specifically for the task of detecting and blocking CSAM on computer devices.

From 2011 to 2014, the CSA filtering set up was hosted at the ICTA and was connected to all local ISPs providing Internet access to the public in Mauritius. After 2014, the CSA shifted to a cloud-based mode whereby no hardware was required anymore at the ICTA premises.

---

[16] After this date, the portal-based reporting system was transferred to CERT-Mauritius (Computer Emergency Response Team of Mauritius, a division of the National Computer Board (NCB) under the aegis of the Ministry of Information Technology, Communication and Innovation.

[17] OECD, "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", *op. cit.,* p. 66.

[18] "Note by the Information and Communication Technologies Authority (ICTA). Child Sexual Abuse (CSA° Filtering Mechanism updates on Child protection Initiative – ITU", Document CWG-COP-18/5-E, ITU Council Working Group on Child Online Protection, 18th meeting – Virtual, 12 January 2022.

[19] Even in this case, Domains and IP addresses can still be reported directly to the IWF online reporting portal (https://report.iwf.org.uk/en) for further action.

Since November 2020, Net sweeper has been the new provider for CSA filtering, using the same cloud-based technology as before.

These effective solutions should be pursued in the future.

However, attention has been drawn to the fact that it has to be noted that the ICTA, as an ICT regulator is involved in regulating ICT infrastructure and services only. As such, the preventive cybersecurity technical solution for CSA deployed for CSA by the ICTA is in line with sections 18 (m) of the ICT Act and section 15 of the Child Protection Act. It is also stressed that ICTA does not get involved in investigatory aspects of CSA.

V. CONCLUSION

Mauritius is signatory to international treaties, for example, Human Rights Convention which include the right of children, whereby, protection of children from all/any kind of harm have been mentioned. The Judiciary and Legal System of Mauritius and concerned stakeholders have to abide and uphold those treaties. Mechanisms to prevent likelihood of such malpractices should be put in place. The Technical Committee looking into the phenomenon of Child/Revenge Pornography could be made into a Standing Committee to review adequacy of measures and propose future measures on a continuous basis. Since institutions would tend to restrict their involvements strictly according to existing legal and institutional frameworks, grey areas may be left effectively unattended resulting in less effective addressing of cases. Future amendments to the existing laws should boldly address such issues to allow for more clearer roles of different institutions and more collaborative approaches.

It's important to acknowledge potential constraints that may affect the comprehensiveness and generalizability of the research findings. While this study focuses on the specific case of Mauritius, the findings and recommendations may not be directly applicable to other regions or countries. The socio-cultural and legal contexts can vary significantly, and therefore, the results may not be generalizable beyond Mauritius. The quality and availability of data related to child and revenge pornography may pose limitations. Some cases and incidents may go unreported, leading to underrepresentation in the analysis. Additionally, variations in data collection and reporting mechanisms may impact the accuracy of the findings.

The study's recommendations and conclusions are based on a comprehensive review of existing literature and available information. However, the perspectives and insights of relevant stakeholders, such as government agencies, law enforcement, NGOs, and legal experts, may not be fully integrated into the findings. Further in-depth interviews or surveys with these stakeholders could provide a more comprehensive understanding.

Finally, this study primarily focuses on legal and institutional aspects. It may not fully encompass the complex interplay of cultural, social, and psychological factors that contribute to the prevalence of child and revenge pornography. A more in-depth analysis of these non-legal aspects could enhance the understanding of the issue.

REFERENCES

Albury, K., Crawford, K., & Byron, P. (2013). Sexting, consent, and young people's ethics: Beyond Megan's Story. *Continuum, 27*(4), 463-473.

Citron, D. K. (2014). Cyber Civil Rights: An Essential Component of Civil Rights in the Twenty-First Century. *Boston University Law Review, 94*(5), 1-61.

Citron, D. K., & Franks, M. A. (2014). Criminalizing Revenge Porn. *Wake Forest Law Review, 49*, 345-391.

Döring, N., Daneback, K., & Shaughnessy, K. (2017). Ethical Dilemmas of Online Research: How Can Researchers Deal with Trolls and Obscene or Abusive Content on Social Media? *Social Media + Society, 3*(1), 2056305117700670.

ICTA (Information and Communication Technologies Authority). (2011). Online Content Filtering (OCF) Solution Implementation.

Information and Communication Technologies Authority (ICTA). (2022, January 12). Note by the Information and Communication Technologies Authority (ICTA). Child Sexual Abuse (CSA) Filtering Mechanism updates on Child protection Initiative – ITU. Document CWG-COP-18/5-E. ITU Council Working Group on Child Online Protection, 18th meeting – Virtual.

International Telecommunication Union (ITU) and United Nations Children's Fund (UNICEF). (2015). Guidelines for Industry on Child Online Protection.

Internet Watch Foundation (IWF). (Year). [Description of the IWF online reporting portal]. Retrieved from https://report.iwf.org.uk/en

ITU. (2020). Guidelines for policy-makers on Child Online Protection. (pp. 32-33).

ITU. (2021, October). Policy brief "Keeping children safe in the digital environment: The importance of protection and empowerment". (p. 6).

Krieger, F., Tymula, A., Glimcher, P. W., Levy, I., & Louie, K. (2017). Neural Signatures of Third-Party Punishment: Evidence from fMRI. *Social Cognitive and Affective Neuroscience, 12*(8), 1209-1217.

MAUCORS (Mauritian Cybercrime Online Reporting System). (2022, May). Cybercrime Incidents Reported to CERT-MU from 2020 to 30 April 2022.

Memorandum of Understanding between Internet Watch Foundation (IWF) and Information and Communication Technologies Authority (ICTA). (2013, October 24).

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2007). Trends in Youth Reports of Sexual Solicitations, Harassment and Unwanted Exposure to Pornography on the Internet. *Journal of Adolescent Health, 40*(2), 116-126.

OECD. (2011, May 2). The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them. *OECD Digital Economy Papers, No. 179*, OECD Publishing, Paris, p. 32. [http://dx.doi.org/10.1787/5kgcjf71pl28-en]

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2007). Unwanted and Wanted Exposure to Online Pornography in a National Sample of Youth Internet Users. *Pediatrics, 119*(2), 247-257.