Reflection on Indonesian Regulations Regarding the Prevention and Enforcement of Sexual Violence Online

Ani Purwanti[1], Dyah Wijaningsih[2], Muh. Afif Mahfud[3]
{ani_purwanti81@yahoo.com[1]}

Universitas Diponegoro, Indonesia[1, 2, 3]

Abstract. Online sexual violence uses digital technology to facilitate virtual and face-to-face sexual crimes. Online sexual harassment, gender and sexuality-based harassment, cyberstalking, image-based sexual exploitation, and using trains to pressure victims into unwanted sexual actions are examples. This page describes Indonesian law-related online/digital sexual violence prevention and eradication. Current cyber-sexual laws solely punish criminals. Indonesia requires legislation defining and preventing sexual frameworks, including cybersexuality. Some cases of cyber attention go unreported, and most reported cases are left unreported due to current legislation. Sexual Violence Crime Law aims to provide legal protection from all forms of sexuality and legal freedom. The statute specifies sexual violence. This law prohibits sexual conduct in different ways, holds parties accountable, protects victims, and restores victims' rights. All parties must prepare this law with seriousness and attention, and it must be enforced with a sense of justice in society and legal certainty for victims. The term "sexual violence in the digital age" describes a pattern of conduct in which people use the internet to commission sexually violent acts against others, both in the virtual and real worlds. Online sexual harassment, harassment based on gender or sexual orientation, cyberstalking, sexual exploitation through images, and forcing people to engage in sexual acts on trains are all examples of this type of activity. This article reflects the present state of Indonesian law regarding preventing and eliminating sexual abuse via online/digital methods. The only thing that can be done to safeguard victims of cyber-sexual assault is to limit the punishment of those who commit such crimes. Moreover, Indonesia needs laws that define and prohibit sexual frameworks, including cybersexuality. Some cases of cyber attention go undetected, and most reported cases are left unreported, given that present legislation does not accommodate this situation. The emergence of the Sexual Violence Crime Law is an effort to provide legal protection to be free from all sorts of sexuality and is formed to realise legal freedom. More specific types of violence, including sexual violence, are defined by the law. This law also includes preventing sexual activity in different ways, holding parties accountable, safeguarding victims, and restoring victims and their rights. As a result, everyone involved needs to take enacting this law seriously and pay close attention to the details. It is vital to enforce the law based on a feeling of justice in society and give legal certainty to the victim.

Keywords: Sexual Violence, Online, Law Enforcement, Literature Study

IWLEG 2022, July 27, Semarang, Indonesia

DOI 10.4108/eai.27-7-2022.2326246

1 Introduction

The term "Online Gender-Based Violence" (OGBV) refers to sexually aggressive and harassing behaviours that are committed with the use of digital communication technology and can be classified as cybercrimes (criminal, civil, or malicious acts) [1]. Perpetrated by those fascinated with the sexuality or gender identity of their victims, OGBV is an assault on the victim's gender identity. It is recognised as a violation of human rights [2, 3, 4]. Teenage girls and young women are particularly vulnerable as a result of this. Stalking, bullying, sexual harassment, defamation, hate speech, and exploitation are all crimes that can be committed using the Internet [5]. Because of this, the International Center for Research on Women also refers to OGBV as Technology-Facilitated Gender-Based Violence or Technology-Facilitated Sexual Violence.

Online Gender-Based Violence (OGBV) refers to cybercrimes that are criminal, civil, malicious, sexually aggressive, or harassing [1]. OGBV violates a person's gender identity and human rights [2, 3, 4] and is committed by those obsessed with their victims' sexual or gender identity. This endangers teenage girls. Stalking, bullying, sexual harassment, defamation, hate speech, and exploitation are committed using the internet [5]. The International Center for Research on Women calls OGBV Technology-Facilitated Gender-Based Violence or Technology-Facilitated Sexual Violence.

Developed countries like the US have failed to address online gender-based violence legislatively despite media and activist pressure. Indonesia's National Commission on Anti-Violence against Women reported a 300% increase in OGBV instances in its 2020 Annual Report. Even during the Pandemic, OGBV cases increased by 400% [6]. SaFENet campaigns for digital rights in Southeast Asia and criticizes OGBV. The study hurts Indonesia's efforts to promote gender equality and give women broadband ICT access. ICT could improve millions of women's health, education, financial status, and community participation. ICT access prevents violence against women and makes the internet safe for women. ICT and internet access will also promote gender equality.

Cyber-VAWG is a global issue that affects society and the economy. Women of a certain religion, ethnic or racial group, sexual orientation, economic background, and disability face online assault globally. 18-24-year-old women are at increased risk for Cyber-VAGW. A quarter of the 4,000 women surveyed in European countries, even the most developed, have experienced online or cyber harassment at least once, according to Amnesty International (2018). 18% of EU women have experienced serious Internet violence since age 15, or 9 million. VAWG includes graphic and threatening texts, emails, photos, and videos. Online dating, social media, chat rooms, and instant messaging are common dispatching platforms. Women and girls of all ages are more likely than men and boys to experience this [7, 8, 9]. Due to contradictory research results, cyberbullying does not appear to be a gender-based cybercrime. The research found gender to be a significant predictor of cyberbullying [10, 11, 12, 13], but others did not [14, 15, 16, 17, 18, 19, 20].

Technology-related gender-based violence impairs women's productivity and capacity to execute daily chores. In such a setting, women withdraw and self-censor, losing contact and employment opportunities [21]. Survivors must also pay for legal fees, health care, relocation, and online removal of their information or photographs [22]. No one lost their homes, property, or social relationships [23]. As new technology and social media platforms emerge, gender-based online violence grows rapidly, endangering women and girls. Online harassment, stalking, and the Pandemic worsen other threats, and current measures are insufficient.

This article reviews Indonesia's policy map on online gender/sexual violence. There is research on gender-based cyber-violence in Indonesia, where it harms society and inhibits efforts to attain gender equality. This study analyses the extent to which gender-based cyber violence has entered Indonesian society and what laws and policies have been enacted to restrict its development.

Despite pressure from the media and women campaigners, wealthy countries like the United States have failed to combat online gender-based violence at the legislative level. According to the 2020 Annual Report published by the Indonesian National Commission on Anti-Violence against Women, the number of cases of OGBV in that country increased by 300 per cent from the previous year. There was a 400% increase in OGBV cases between the Pandemic and 2019 [6]. SaFENet (Southeast Asia Freedom of Expression Network) is a non-governmental organisation (NGO) that promotes online freedom of expression and condemns online gender-based violence (OGBV) in Southeast Asia. The report undermines Indonesia's attempts to advance gender parity and expand women's access to high-speed Internet in various fields. Millions of women are expected to benefit from ICT in terms of improved health, education, economic standing, and social engagement. Having access to information and communication technologies will also reduce the risk of sexual assault and make the Internet a more welcoming place for women. Lastly, advancements in information and communication technology and widespread internet access will usher in a new era of gender parity.

Cyber-VAWG, or cyber violence against women and girls, is a growing problem with far-reaching consequences for individuals, communities, and nations. There are many sorts of cyberbullying that affect women around the world. The women who fall into these categories are members of specific religious communities, racial and ethnic minorities, sexual minorities, socioeconomic classes, and demographics. In particular, young adult women (those aged 18–24) are at significant risk for getting any Cyber-VAGW. Amnesty International (2018) found that 24% of 4,000 European women surveyed have experienced online or cyber harassment at least once. This includes women from the most developed European countries, such as the USA, the UK, Spain, and Italy. About 9 million European Union women, or 18% of all women, have experienced serious Internet violence since 15. Sexually graphic or threatening texts, emails, photos, or videos are all forms of VAWG. Some of the most common dissemination platforms are online dating sites, social media sites, and chat rooms/IM services. This abuse is more common among women and girls of all ages than it is among men and boys [7, 8, 9]. Research on the role of gender in cyberbullying has shown contradictory results, suggesting that cyberbullying is not a cybercrime that is more prevalent among one gender. Although some research [10, 11, 12, 13] and others revealed that gender was a significant predictor of cyberbullying, others did not [14, 15, 16, 17, 18, 19, 20].

There is a global correlation between acts of violence against women and the use of technology, which hurts women's capacity to work and fulfil their daily chores. Women tend to shut down and self-censor when put in such a position. They stop talking to people and have trouble finding work because of it [21]. They lose money and, as survivors, have to pay a lot for things like legal help, medical care, relocating, and getting their names and photos scrubbed from the Internet [22]. None of them had to abandon their homes, possessions, or social networks [23]. Because of the rise of new technologies and online communities, cyberbullying is on the rise, posing a serious threat to the security of women and girls. Changes in the online environment during the Pandemic have a multiplier effect on forms of cyberbullying such as cyber stalking, and current responses are insufficient to stem the tide.

Using a literature review approach, this essay examines Indonesia's current policy terrain regarding gender/sexual violence in cyberspace. While sexual and gender-based cyber-violence harms Indonesian society and hamper government efforts to achieve gender equality, little research has focused on this issue in the context of Indonesia. Consequently, this study seeks to address this knowledge gap by examining the prevalence of gender-based cyber violence in Indonesian society and the efficacy of the laws and regulations to prevent its further development.

2 Literature Review

Cyberbullying based on gender can take many forms, including unwanted sexual comments and images, posting sexual content without the victim's consent, impersonation, hacking, spamming, tracking and surveillance, making malicious threats, and harassing someone through gender-based discriminatory photos and posts. Cyberstalking, non-consensual pornography (also known as "revenge porn"), gender-based insults, hate speech and harassment, "prostitute humiliation," unsolicited pornography, "sextortion," rape and death threats, and electronically facilitated trafficking are some of the forms of cyber violence that can be committed against women and girls. These are just some forms of cyber violence that can be committed against women and girls. Women in Ghana are subjected to harassment online through sexually explicit photographs and videos and rude comments [24]. Many studies report instances of gender-based harassment from different parts of the world [1, 25, 26]. Cyberstalking and harassment have also been directed at feminist organisations and individuals fighting for women's rights. As an illustration, in Colombia, there have been reports of sexual aggression and stalking of women's activities that took place online [27]. Even though being a female public person makes one more susceptible to sexual harassment and misogynistic comments online, as was documented by UK Labor MP Jess Phillips, who got more than 600 rape threats in one night and nasty comments on her internet account [28]. Women and young girls, men, boys, and other identities across racial and religious lines are included in the category of vulnerable groups. Using information and communication technology (ICT) means "to promote or extend sexual and gender-based harm to victims," including "technology-enabled assault," is what Powell and Henry [1] mean when they refer to online gender-based cyberbullying as "technology-facilitated sexual violence." sexual harassment; image-based sexual harassment; online sexual harassment; cyberstalking and criminal harassment; gender-based harassment and hate speech" [1, 29]. The Association for Progressive Communications (APCCinco)'s [30] asserts that "violence against women is changing due to the reason of technology" and that "the Internet has opened up private life into new potential avenues of violence." She also states that "the Internet has opened up private life into new potential avenues of violence."

Online gender-based cyberbullying includes unwelcome sexual comments, publishing sexual media without consent, impersonation, hacking, spamming, tracking and surveillance, malicious threats, and discriminatory photographs and posts. Cyberstalking, non-consensual pornography ("revenge porn"), gender-based insults, hate speech and harassment, "prostitute humiliation", unsolicited pornography, "sextortion", rape and death threats, and electronically assisted trafficking are all kinds of cyber violence against women and girls. In Ghana, women are harassed online with sexually explicit photographs and videos [24]. Several studies describe gender-based harassment worldwide [1, 25, 26]. In Colombia, online sexual aggression and stalking of women's activities were recorded [27]. As a female public personality, Jess Phillips received more than 600 rape threats in one night and abusive comments online [28]. Women, girls, men, and different ethnicities and religions are vulnerable. Powell and Henry [1] call online gender-based cyberbullying "technology-facilitated sexual violence" that uses ICT "to facilitate or prolong sexual and gender-based harm to victims," including, "technology-enabled assault." cyberstalking and criminal harassment; sexual harassment; online sexual harassment; gender-based harassment; hate speech" [1, 29]. Cinco [30] of the Association for Progressive Communications (APC) says "violence against women is changing because to technology" and "the Internet has brought up new possible routes of violence."

Sexual harassment online is increasing, and cases are becoming more complex, with perpetrators and victims often hidden. Some cyber sexual harassment victims did not report it. This is because access to justice for victims is impeded or not through the legal system. The present legal protection is restrictive, meaning it has not granted total victims, particularly women. However, additional legal protection is needed. The regulation must encompass offender punishment and victim protection, including prevention, protection, handling, and recovery.

Along with every goal and purpose, internet sexual harassment victims can achieve justice. Moreover, material and formal legislative restrictions must be amended because they lack a framework for victim prevention, protection, and handling. The Law on the Elimination of Sexual Violence has a deterrent impact and cuts abusers' impunity, preventing recurrences.

Digital abuse, cyberstalking, and cyberbullying are often used interchangeably in the study. Empirical research refers to "electronic aggression" [31], "electronic harassment" [32], and "online harassment" [33, 34]. Few empirical investigations have focused on online victimisation and sexual aggressiveness or coercion. Thompson dan Morrison [35] called digitally-based sexual behaviour "technology-based coercive behaviour" (e.g., requesting sexual information online, sending sexually provocative messages, photographs, etc.). Gamez-Guadix et al. [36] define "online victims" as "pressure to acquire unwanted sexual collaboration or the dissemination of victims" sexual content via the Internet. Reyns et al. [9] adopt Marcum et al. [37]'s phrase "cyber victimisation" to refer to sexually graphic images, harassment, and sexual solicitation. Empirical investigations of digital violence tend not to define distinct behaviours into independent aspects, and "online sexual harassment" [38] or "cyber-harassment" [39] acts as a general term. Digital aggression or sexual harassment categories. This article differentiates between behaviours using five overlapping dimensions.

This dimension includes unwelcome sexual attention, speech acts, fear-inducing activities, image-based violations, and bodily violations/contacts. Categorising this behaviour enables better legal responses, legislation, and prevention. Egalitarian and prosperous criminal justice must respond differently to victims and various criminals. Other scholars that study harassment and online harassment do not focus on sexual or gender violations, even though they may include sexual-based behaviour. Sexuality and non-sexuality are not always explicit. One example is intimate relationship cyberstalking, where the offenders utilise GPS tracking to manage and supervise their victims. Calling someone sexual or gender-demeaning terms (such as "prostitutes") may not be online sexual harassment if done with good intentions (for example, in comedy sketches or as jokes among friends). Second, despite the tight relationship between sexuality and gender, not all digital harassment is "sex." Widespread mass harassment of a female blogger may not be gender-based harassment unless sex is the incentive (or "Bias Motivation").

Existing statutes on stalking, sexual harassment, and hate speech guide difference construction. The article's dimensions are based on legal definitions and are not problematic.

The conditions are that an act is undertaken because of a person's or a group's gender or sexual orientation and is done to harm and cause considerable harm to the victim; losses that may (or may not be) expressly "sexed". This does not mean the perpetrator's reasons are entirely based on gender or sexuality. However, such behaviour is partially the result of gender inequalities and hierarchies, which form normative expectations around femininity and masculinity [40]. This gender hierarchy allows for more variety and complexity in deeds and victims. First, it recognises that men, boys, and transgender people are victims of TFSV and offenders. Second, this framework permits a complete analysis of masculinity and femininity in online and offline environments, including the gender implications of these behaviours and the confluence of marginalisation based on age, race, religion, ethnicity, sexuality, and sex. With this distinction in mind, many online behaviours can be omitted from the cyber sexual/gender category, such as vandalising a Facebook memorial page or cyber harassment, cyberstalking, and hate. Non-sexual assault or gender-based harassment-related speech. This gender hierarchy allows for more variety and complexity in deeds and victims. First, it recognises that men, boys, and transgender people are victims of TFSV and offenders. Second, this framework permits a complete analysis of masculinity and femininity in online and offline environments, including the gender implications of these behaviours and the confluence of marginalisation based on age, race, religion, ethnicity, sexuality, and sex. With this distinction in mind, many online behaviours can be omitted from the cyber sexual/gender category, such as vandalising a Facebook memorial page or cyber harassment, cyberstalking, and hate. Non-sexual assault or gender-based harassment-related speech.

The number of incidents of sexual harassment committed in cyberspace continues to rise, as does the complexity of the cases that involve these incidents. In particular, the problem of sexual harassment in cyberspace and the identities of those harassed online are kept secret. There were victims of sexual harassment in cyberspace who did not report the incident, and there were also victims who did not report the incident. This is because access to justice for victims is indeed hindered or not through the legal system, and the existing legal protection is repressive, which means that it has not given full victims of victims, particularly women. This is because access to justice for victims is indeed hampered or not through the legal system. In any case, there is a requirement for additional, comprehensive legal protection associated with the issue. The legislation must not only govern punishments for the people who committed the crime, but it must also regulate protections for the victims, such as the prevention of victimisation, protection, treatment, and recovery. In addition to a reference to all of the intent and purpose of providing victims of online sexual harassment with the right or access to justice, these victims can also get the right. In addition, legislative rules are complete, including both material and formal legislation; however, they need to be amended, and they have not created a framework for the prevention of crimes, protection of victims, and the resolution of favourable cases to victims. In addition, the Law on the Elimination of Sexual Violence can continue to have a preventative effect and reduce the impunity afforded to those who commit sexual violence. As a result, there will be no further instances of crime.

In the larger body of research literature, the phrases digital abuse, cyberstalking, and cyberbullying are often referred to using various terms that are interchangeable. Empirical research, for instance, refers to a group of behaviours by using names like "electronic aggression" [31], "electronic harassment" [32], and "online harassment" [33, 34], respectively. These phrases are used to describe electronic forms of harassment. Only a handful of empirical studies have specifically focused on the crossover between sexual aggressiveness or coercion that occurs online and online victimisation. In their analysis of digitally-based sexual behaviour, Thompson and Morrison [35] used the term "technology-based coercive behaviour." Some examples of this behaviour include asking for sexual information about someone online, posting sexually suggestive messages or pictures to someone's online profile, and many other similar activities. According to Ga'mez-Guadix et al. [36], the term "online victims" refers to people who have been subjected to "pressure to acquire unwanted sexual collaboration or the publication of sexual content of victims via the Internet." The phrase "cyber victimisation" comes from the work of Marcum et al. [37], and it is used by Reyns et al. [9] to refer to the act of accepting sexually explicit photographs, as well as harassment and sexual solicitation. These empirical investigations of digital violence have a tendency not to classify diverse acts into independent dimensions, and "online sexual harassment" [38] or "cyber-harassment" [39] frequently serves as nothing more than a general term. A categorisation of the various forms of sexual harassment or acts of physical assault can occur online. Nevertheless, this essay aims to differentiate between the various behaviours by referring to five aspects that overlap with one another.

This dimension encompasses harassment or violence, including unwelcome sexual attention, speech acts that generate terror or fear, image-based violations, or physical violations/contacts. Additionally, this dimension may also include image-based violations. This classification is appropriate because it makes it possible to develop more effective legal responses, policies, and preventative measures for a wider range of behaviours. However, the impact on victims is distinct between these various dimensions, the people who commit one behaviour are not the same as the people who commit the other behaviour, and the response of the criminal justice system must respond differently to various victims and perpetrators in order to be fair, equal, and effective. Other researchers that look into harassment and online harassment typically do not place much emphasis on the risks associated with sexual or gender violations, even though both types of harassment can include various aspects based on sexually-based conduct. There is frequently a blurring of the lines between sexual and non-sexual behaviours. One example is a form of cyberstalking known as "intimate relationship cyberstalking," in which the offenders utilise technology to control and monitor their victims, such as by tracking their global position system (GPS).

Another example is referring to a person using derogatory terms based on their gender or sexual orientation (such as "prostitutes"), which might not be considered a form of online sexual harassment if it is done with positive intentions (for example, in comedy sketches or as jokes among friends). Second, despite the close connection between sexuality and gender, all forms of online harassment need not be of the "sex" variety. For instance, the widespread and mass harassment of a female blogger could not always be considered a type of harassment based on the victim's gender. Unless sexualities were the reason or motivation for the harassment, it would be referred to as "Bias Motivation."

Existing laws on stalking, sexual harassment, and hate speech in offline contexts provide useful information on how to create differences, even though there are ambiguous distinctions that call for more examination. The legal definitions used as a model for the dimensions described in this article are not necessarily problematic in and of themselves. The act must have been committed for the reason that the gender or sexual orientation of a person or some or all of the people in a group, and it must have been accomplished to hurt, and it must have caused significant harm to the victim; losses that may (or may not be specifically "sexed"). The victim's losses may (or may not be specifically "sexed"). This does not mean that the perpetrator's motivations must be specifically or solely based on gender or sexuality; rather, it indicates that such behaviour is partially the result of a context of gender inequality and hierarchies, which in turn shape normative expectations around femininity and masculinity [40]. This concept of a gender hierarchy makes it possible to capture greater richness and complexity in terms of both acts and victims. In the first place, it makes it possible to acknowledge that men, boys, and transgender persons can be victims of TFSV as well, in the same way as women and other transgender people can be perpetrators of the behaviour. Second, this conceptualisation makes it possible to conduct an in-depth study of the social constructions of masculinity and femininity in both online and offline settings, including the gender impact of certain behaviours and the complex ways in which marginalisation based on age, race, religion, ethnicity, sexual orientation, and sex can interact with one another.

Along with keeping this essential distinction in mind, a wide range of online behaviours can, without a doubt, be excluded from the cyber sexual/gender classification. These behaviours include people vandalising the Facebook memorial page of a deceased person as well as other forms of cyber harassment, cyberstalking, and hate speech. Speech that does not expressly or implicitly connects to sexual assault and harassment based on sexual orientation and gender. This concept of a gender hierarchy makes it possible to capture greater richness and complexity in terms of both acts and victims. In the first place, it makes it possible to acknowledge that men, boys, and transgender persons can be victims of TFSV as well, in the same manner as women and transgender people can engage in the behaviour. Second, this conceptualisation makes it possible to conduct an in-depth study of the social constructions of masculinity and femininity in offline and online settings, including the gender impact of certain behaviours and the complex ways in which marginalisation based on age, race, religion, ethnicity, sexual orientation, and sex can interact with one another.

Along with keeping this essential distinction in mind, a wide range of online behaviours can, without a doubt, be excluded from the cyber sexual/gender classification. These behaviours include people vandalising the Facebook memorial page of a deceased person as well as other forms of cyber harassment, cyberstalking, and hate speech. Speech that does not directly or implicitly connect to sexual assault or other forms of harassment based on gender or sexuality.

3 Methodology

This article is normative legal research that uses a literature study approach to examine the condition of Indonesia's policies in dealing with online gender-based sexual violence.

4 Discussion

By the International Convention on the Elimination of All Forms of Discrimination against Women, which Indonesia signed and ratified in 2000, the Indonesian constitution guarantees unequivocally gender equality (CEDAW). The Presidential Instruction on Gender Mainstreaming was ratified at the convention. As a result, it mandates that all ministries and government agencies, on both the national and local levels, give gender mainstreaming the priority it deserves in all development programmes. The Ministry of Finance distributes a paper titled Gender Equality and Diversity (GED) to all government units with the recommendation that they establish a GED task force to ensure the successful implementation of gender mainstreaming. In order to formulate a strategy for achieving gender equality, this task force should be made up of high-ranking government officials who will be tasked with the role of

"Gender Champions" with the members of that role. It is an excellent example of compliance with GED regulations that the Indonesian Department of Customs and Excise developed the Gender Equality Organizational Assessment Tool (GEOAT) to assess whether or not existing policies and procedures on gender equality comply with GED norms. This action was taken to determine whether existing policies and procedures on gender equality comply with GED norms. In addition to this, they developed an analytical instrument that they named the Gender Analysis Pathway (GAP) in order to investigate the areas in which advancements are necessary to attain gender equality. As a result of all of these efforts, there is no question that Indonesia has launched a programme to promote gender equality in the country. This is also evident in improved literacy rates, school enrollment rates, and employment rates, in addition to women's empowerment laws, which suggest a more gender-just society. The national parliament approved an anti-pornography law in 2008, and its passage contributed to reducing violence against women, particularly online and cyberbullying.

The 2000 International Convention on the Elimination of All Forms of Discrimination against Women confirmed the Indonesian constitution's gender equality guarantee. The convention passed the Presidential Instruction on Gender Mainstreaming, which compels all national and local ministries and agencies to mainstream gender in all development programmes. The Ministry of Finance distributes a document called Gender Equality and Diversity (GED) to all government units to establish a GED task group to ensure gender mainstreaming. This task force should include "Gender Champions" and their members to establish a Gender Equality action plan. The Indonesian Department of Customs and Excise developed the Gender Equality Organizational Assessment Tool (GEOAT) to analyse whether gender equality policies and procedures meet GED principles. They also created the Gender Analysis Pathway (GAP) to examine where gender equality needs development. Indonesia has launched a gender equality initiative based on these efforts. Increased literacy, school enrollment, employment, and women's empowerment programmes signify a more gender-just society. In 2008, the national parliament established an anti-pornography law to ban the internet and cyber bully.

This law advances gender equality. The National Commission on Violence Against Women reported an upsurge in violence against women during COVID-19, mainly due to internet and ICT overexposure. The government is considering passing an anti-sexual violence law in light of the SDGs. Indonesia's SDG gender equality indices are moderately improving,' but there remains a long way to go socially and politically. The country's gender equality goal is 2030. The National Commission on Violence Against Women agreed to explore online gender-based violence in response to global demand. They have identified gender-based cyber violence in the digital age. Indonesia's National Commission on Violence Against Women declared cyber violence an increasing trend. Their 2017 annual report highlighted online defamation, malicious distribution, privacy invasion, illicit content, hacking, cyber harassment, and cyber grooming. These categories marginalise women since they are easy victims, signalling continuing inequality in Indonesian society despite efforts to promote gender equality. Indonesian law devotes little attention to preventing online harassment; loopholes and anomalies encourage criminals. Indonesia's Information and Electronics Law allow suspects to report defamation victims. Thus, the victim and perpetrator are combined. Victims do not consider the implications of revealing their identities and sharing their experiences, not realising that the law itself could be defamatory.

In essence, Indonesia's Sexual Violence Crime Law addresses this issue. The Sexual Violence Crime Law is critical in the battle against sexual violence because sexual harassments continue to rise. The existing legal system has not consistently and fully structured prevention, protection, and recovery of victims, nor has it raised public awareness of the issue. The Sexual Assault Crime Law also emphasises the need to prevent sexual violence, hold parties accountable, and safeguard victims' rights. The Sexual Violence Crime Law also regulates sexual harassment. Physical and non-physical sexual harassment is illegal under the Sexual Violence Crime Law. Cybersexual harassment is non-physical. Article 91 of the Sexual Violence Crime Law states: "People who commit non-physical sexual harassment are penalised with special rehabilitation for a month and social work."

Sexual harassment victims undergoing a mental shock have additional protections. Article 94 of the Sexual Violence Crime Law states, "Victims of sexual harassment who experience mental shock, perpetrators are sentenced to a minimum of four years and a maximum of eight years, and additional particular coaching." The scope that must be covered in the formation of a new national law that applies the concept of progressive law is: First, enactment of online sexual violence as a joint action with particular procedural provisions (one of which is the enactment of courts for online based sexual violence and violence cases). This is the initial step for further law enforcement since online-based sexual assault actions are undesired, harmful to society, and counter to Indonesia's goals. Hence they have been criminalised. Criminalising sexual violence can help criminalise online sexual violence. Article 5 of the House-approved Sexual Violence Crime Law addresses sexual harassment via technological means. Article 5, paragraph 1 of the Sexual Violence Crime Law exclusively covers sexual harassment. Therefore, the authors argue: It is necessary to emphasise online-based sexual violence as one of the separate acts of sexual violence in the Sexual Violence Crime Law and the classifications included in it as a crime to accommodate numerous forms of online-based sexual violence and consider that the management of online-based sexual violence online is preeminent due to the use of technology platforms and service providers, and after the implementation of the first recommendation. They were second, maximising victims' rights, including the right to be forgotten. This is done by synchronising national laws with ESO user policies/guidelines (ESP). Implementing the right to be abandoned can optimise the special rights of victims of online-based sexual violence in two ways: First, victims of online-based sexual violence can ask the state to remove their sexual content through a court order. This practice was ended in the EU by Case C-131/12 of 2014. Alternatively, the new legal norm can include the right to be abandoned.

The passage of this law further advances their efforts toward achieving gender equality. The National Commission on Violence Against Women reported an increased incidence of violence against women during COVID-19. The primary cause of this increase was excessive exposure to the internet and other ICT gadgets. At this moment, the government is discussing the possibility of enacting a law to combat sexual violence with the Sustainable Development Goals (SDGs) in mind. In terms of gender equality, Indonesia is making "modest improvements" to its SDG indicators, but there is still a significant distance to travel, both socially and politically. The year 2030 is the target date for the nation's goal of achieving gender equality. The National Commission on Violence Against Women has committed to conducting a research study on online gender-based violence in response to a global demand to take action against gender-based cyberbullying. This demand resulted from a global campaign to stop gender-based cyberbullying. Their efforts successfully identified gender-based online violence prevalent in this day and age of digital technology. The National Commission on Violence Against Women in Indonesia was put in the position of acknowledging that cyber violence is a growing trend targeting women. In their annual report for 2017, they noted several types of cyberbullying, including online defamation, malicious distribution, invasion of privacy, illegal content, hacking, cyber harassment, and cyber grooming. These categories not only marginalise women because they make them easy targets for victimisation, but they also signify the growing inequality that persists in Indonesian society despite the many efforts that have been made over the years to bring about gender equality. The prevention of online harassment receives very little attention in Indonesian legislation; in fact, several loopholes and anomalies allow criminals more courageous to commit crimes. For instance, Indonesia's Information and Electronics Law protect individuals who may have violated the law by enabling them to file defamation complaints on behalf of victims. By doing it this way, both the victim and the offender are lumped into the same category. Consequently, victims fail to properly weigh the benefits and drawbacks of publicising their names and discussing their experiences because they are unaware that the law itself may be a source of more slander.

Indonesia already has a discourse on this issue, which can be observed in the provisions of the Sexual Violence Crime Law. This discourse may be found in Indonesia. Because the number of incidents of sexual harassment continues to rise, the passage of the Sexual Violence Crime Law was an essential step in the fight against sexual violence. This is because the number of people subjected to sexual harassment is growing. Despite this, the existing legal system has not been arranged in a systematic or comprehensive way. They are prevention, protection, and recovery for victims; however, public awareness has not been supplied regarding this subject. The Sexual Violence Crime Law draws attention to the necessity of preventing sexual violence in various contexts, holding responsible parties accountable, protecting and rehabilitating victims, and recovering victims' rights, among other things.

Additionally, the Sexual Violence Crime Law controls particular specific types of violence, such as sexual harassment, in addition to the more general forms of violence. The Sexual Violence Crime Law classifies sexual harassment as physical or non-physical. These two categories are known as physical and non-physical sexual harassment, respectively. Sexual harassment that does not include physical contact is known as cybersexual harassment. Article 91 of the Sexual Violence Crime Law contains the following provisions about non-physical sexual harassment: "People who conduct acts of non-physical sexual harassment are penalisedpenalised with special rehabilitation for a maximum of one month and social work." There are further requirements regarding how victims of sexual harassment should be treated if they experience mental shock. This statement can be found in Article 94 of the Sexual Violence Crime Law: "victims of sexual harassment who experience mental shock, perpetrators are sentenced to a minimum of four years and a maximum of eight years, and additional particular coaching." The scope that must be covered in the formation of a new national law that applies the concept of progressive law in it is as follows: First, enactment of online sexual violence as a joint action with particular procedural laws to deal with the repercussions of such violence (one of which is the enactment of courts for online based sexual violence and violence cases). This is the first step toward additional law enforcement because acts of sexual violence committed through the internet are unacceptable, harmful to society, and run counter to the objectives of the Indonesian national government. As a result, they have satisfied the conditions necessary for criminality. The criminalisation of sexual violence can serve as a starting point for the criminalisation of sexual violence that occurs online. At this point, Article 5 of the Sexual Violence Crime Law, which the house of representatives has passed, has rules regarding sexual harassment by internet means. Despite this, the scope of sexual harassment is the sole offence that can be prosecuted under paragraph 1 of Article 5 of the Sexual Violence Crime Law. Therefore, the authors argue that it is necessary to emphasise the existence of online-based sexual violence as one of the separate acts of sexual violence in the Sexual Violence Crime Law and the classifications included in it as a crime to accommodate numerous forms of online-based sexual violence and that it is necessary to consider that the management of online-based sexual violence online is preeminent due to the reason that it involves the use of technology platforms and service providers. The Sexual Violence Crime Law must be enacted as soon as possible (after implementing the first recommendation).

Second, maximising the fulfilment of the special rights of victims of online-based sexual violence, notably applying the principle of the right to be forgotten by those whom such individuals have harmed in the past. This is accomplished by emphasising synchronisation between individual nations' laws and the user policies and user guides of each Electronic System Operator (ESP). Two approaches can be used in order to accomplish the goal of maximising the fulfilment of the victims of online-based sexual violence's specific rights through the application of the principle of the right to be abandoned: To begin, victims of online-based sexual abuse have the legal right to request that the state remove any of their sexual content that the perpetrators of such violence are unlawfully exploiting. This request must be made through a court ruling. This practice has been put to rest throughout the European Union due to the jurisprudence handed down by the European Union Court of Justice in Case No. C-131/12 of 2014. Another possibility is to incorporate the contentious question of the right to be abandoned as a part of the new legal norm.

5 Conclusion

The growth of digital technology has significantly influenced the pattern of social life, and one of the unintended consequences of this growth is the destructive use of online technology as a tool for cybercrime. In the case of sexual violence committed online against children, cyberspace also influences criminal behaviours by exploiting technology as a foundation for criminal activity. The primary finding was that sexual violence committed against children in cyberspace could psychologically impact children, specifically a sense of trauma and feelings of powerlessness from children. This was presented as the finding. As a result, children will continue to mature and advance over time. There is no specific regulation regarding crimes threatened by perpetrators of child sexual violence in cyberspace in the ITE Law in Indonesia; instead, it only mentions cyber pornography in general. This is because there is no specific regulation regarding child sexual violence in cyberspace. Therefore, in some criminal instances involving child sexual assault in cyberspace, the regulations that limit the transmission of immoral information are the only ones that can be used as evidence. As a result, the law treats juvenile victims in the same manner as it does adults. Theoretically, this research strengthens the existing laws and regulations on cybercrime in Indonesia by theoretically considering the impact these crimes have on the development of children. Additionally, this research aims to deter perpetrators and prevent crimes like those already committed. Because of these results, it is reasonable to believe that the government will play an active role in maintaining its protection and aid programmes for the victims' psychological recovery.

Cybercrime results from the growth of digital technology, which significantly impacts social life. Cybercrime and sexual assault against children also use technology as a criminal base. Sexual violence done to children in cyberspace can psychologically influence children, primarily through trauma and powerlessness, so children grow and develop. In Indonesia's Information and Electronic Transactions Law, there is no restriction regarding child sexual violence in cyberspace, simply cyber pornography. In criminal prosecutions, some instances of child sexual violence in cyberspace exclusively use immorality laws. The law is the same as for adults. Theoretically, this research strengthens Indonesia's cybercrime legislation by evaluating the impact of these crimes on child development and tries to discourage perpetrators and prevent similar crimes. These results suggest that the government should continue providing victims with psychological aid.

Current cyber-sexual harassment laws solely punish abusers. Indonesia needs a law that defines and bans sexual harassment, including cyberbullying. Some incidences of cybersexual harassment go unreported, and most reported cases are left unreported since laws do not address this issue. Sexual Violence Crime is an effort to retain legal protection from sexual harassment and fills a legal gap. The law defines violence, including sexual harassment. This law emphasises the need to avoid sexual harassment in various ways, include obligated parties, protect victims, and restore victims' rights. All parties must take this law seriously and pay attention to its details to provide victims with social fairness and legal certainty.

The existing legal system that protects victims from cyber-sexual harassment merely controls the penalty of those who abuse others online in this manner. Indonesia needs a specific legislative framework that identifies and prevents sexual harassment in all its forms, including sexual harassment in cyberspace. Given that regulations do not currently make allowances for this problem, there are instances of cyber sexual harassment that are not reported, and the majority of cases that are reported are therefore left unreported. Establishing the Sexual Violence Crime Law is an effort to preserve legal protection to be free from all types of sexual harassment. It is as well-formed as it is because it is to fill a legal vacuum, which is why it is a legal protection to be free from all forms of sexual harassment. The statute specifies additional forms of violence, including sexual harassment, in greater detail. This law brings attention to the necessity of preventing sexual harassment in various methods, including parties that are obligated to do so, protecting victims, and restoring victims' rights. Therefore, preparing for the establishment of this law requires seriousness and attention from all parties. It is required to enforce the law based on a sense of justice in society and to ensure legal certainty for victims.

References

[1] Powell, A., & Henry, N. (2017). *Sexual violence in a digital age*. Springer.

[2] International, A. (2018). Toxic Twitter: A Toxic Place for Women. *Report*.

[3] Lewis, R., Rowe, M., & Wiper, C. (2017). Online abuse of feminists as an emerging form of violence against women and girls. *British Journal of Criminology*, *57*(6), 1462–1481.

[4] UNHRC. (2018). HRC/39/6 (2018): Report of the Working Group on the Universal Periodic Review: Colombia. *United Nations General Assembly*.

[5] Hinson, L., Mueller, J., O'Brien-Milne, L., & Wandera, N. (2018). *Technology-facilitated gender-based violence: What is it, and how do we measure it?*

[6] Ratnasari, E., Sumartias, S., & Romli, R. (2021). Social Media, Digital Activism, and Online Gender-Based Violence in I Indonesia. *Nyimak: Journal of Communication*, *5*(1), 97–116.

[7] Davis, N., & Schmidt, C. (2016). Cyberbullying and cyber abuse intervention: The three-tiered model for schools. *Journal of Creativity in Mental Health*, *11*(3–4), 366–377.

[8] Moriarty, L. J., & Freiberger, K. (2008). Cyberstalking: Utilizing newspaper accounts to establish victimization patterns. *Victims and Offenders*, *3*(2–3), 131–141.

[9] Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149–

1169.

[10] Beran, T., & Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. *Journal of Educational Computing Research*, *32*(3), 265.

[11] Kowalski, R. M., & Limber, S. P. (2007). Electronic bullying among middle school students. *Journal of Adolescent Health*, *41*(6), S22–S30.

[12] Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum*, *32*(1), 81–94.

[13] Navarro, J. N., & Jasinski, J. L. (2013). Why girls? Using routine activities theory to predict cyberbullying experiences between girls and boys. *Women & Criminal Justice*, *23*(4), 286–303.

[14] Calvete, E., Orue, I., Estévez, A., Villardón, L., & Padilla, P. (2010). Cyberbullying in adolescents: Modalities and aggressors' profile. *Computers in Human Behavior*, *26*(5), 1128–1135.

[15] Fanti, K. A., Demetriou, A. G., & Hawa, V. V. (2012). A longitudinal study of cyberbullying: Examining riskand protective factors. *European Journal of Developmental Psychology*, *9*(2), 168–181.

[16] Livingstone, S., Stoilova, M., & Kelly291, A. (2016). 14. Cyberbullying: incidence, trends and consequences. *Ending the Torment: Tackling Bullying from the Schoolyard to Cyberspace*, 115.

[17] Rivers, I., & Noret, N. (2010). Participant roles in bullying behavior and their association with thoughts of ending one's life. *Crisis: The Journal of Crisis Intervention and Suicide Prevention*, *31*(3), 143.

[18] Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. *Computers in Human Behavior*, *29*(1), 26–32.

[19] Smith, P., Caputi, P., & Crittenden, N. (2012). A maze of metaphors around glass ceilings. *Gender in Management: An International Journal*.

[20] Smith, P. K., Mahdavi, J., Carvalho, M., & Tippett, N. (2006). An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying. *Research Brief No. RBX03-06. London: DfES.*

[21] International, A. (2018). Toxic Twitter: A Toxic Place for Women. *Report*.

[22] Dunn, S. (2020). Technology-facilitated gender-based violence: An overview. *Suzie Dunn," Technology-Facilitated Gender-Based Violence: An Overview"(2020) Centre for International Governance Innovation: Supporting a Safer Internet Paper*, *1*.

[23] OHCHR. (2018). *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*. https://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/SRWomenIndex.aspx

[24] Abissath, M. (2018). *Operation Vanguard: A timely saviour of our environment*.

[25] Li, Q. (2006). Cyberbullying in schools: A research of gender differences. *School Psychology International*, *27*(2), 157–170.

[26] Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior*, *23*(4), 1777–1791.

[27] Lyons, M., & Blanchard, A. (2016). "I could see, in the depth of his eyes, my own beauty reflected": Women's assortative preference for narcissistic, but not for Machiavellian or psychopathic male faces. *Personality and Individual Differences*, *97*, 40–44.

[28] Rawlinson, K. (2018). Pressure grows on PM over Brexit Cambridge Analytica scandal. *The Guardian*, *26*.

[29] Powell, A., Henry, N., & Flynn, A. (2018). Image-based sexual abuse. In *Routledge handbook of critical criminology* (pp. 305–315). Routledge.

[30] Cinco, C. (1999). *Asian Women's Resource Exchange*.

[31] Bennett, D. C., Guran, E. L., Ramos, M. C., & Margolin, G. (2011). College students' electronic victimization in friendships and dating relationships: Anticipated distress and associations with risky behaviors. *Violence and Victims*, *26*(4), 410–429.

[32] Fenaughty, J., & Harré, N. (2013). Factors associated with distressing electronic harassment and cyberbullying. *Computers in Human Behavior*, *29*(3), 803–811.

[33] Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence*, *19*(4), 468–483.

[34] Lindsay, M., Booth, J. M., Messing, J. T., & Thaller, J. (2016). Experiences of online harassment among emerging adults: Emotional reactions and the mediating role of fear. *Journal of Interpersonal Violence*, *31*(19), 3174–3195.

[35] Thompson, M. P., & Morrison, D. J. (2013). Prospective predictors of technology-based sexual coercion by college males. *Psychology of Violence*, *3*(3), 233.

[36] Gámez-Guadix, M., Almendros, C., Borrajo, E., & Calvete, E. (2015). Prevalence and association of sexting and online sexual victimization among Spanish adults. *Sexuality Research and Social Policy*, *12*(2), 145–154.

[37] Marcum, C. D., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2010). Policing possession of child pornography online: Investigating the training and resources dedicated to the investigation of cyber crime. *International Journal of Police Science & Management*, *12*(4), 516–525.

[38] Barak, A. (2005). Sexual harassment on the Internet. *Social Science Computer Review*, *23*(1), 77–92.

[39] Citron, D. K. (2014). *Hate crimes in cyberspace*. Harvard University Press.

[40] Connell, R. W. (1987). *Gender and Power*. Polity Press.