ISSN: 3123-6073

CyberShield Technology: Innovation of FaceID-Based Technology in Preventing the Spread of Sexual Content

Agdelia Meiva Azarine
Undergraduate Students – Law Study Program University of Indonesia
email: amazarine19@gmail.com

Joya Josephine
Undergraduate Student – Law Study Program, University of Indonesia
email: dohawangi@gmail.com

Abstrak

This study focuses on discussing the distribution of non-consensual intimate content or non-consensual dissemination of intimate images (NCII) as a form of Online Gender-Based Violence (KBGO). The increasing use of technology has added a new dimension to cybercrime. The mode of distributing sexually nuanced videos belonging to victims has had a negative impact on their psychology. By using analytical descriptive methods and conceptual approaches, statutory approaches, and comparative approaches, this study aims to determine the relevance of the term revenge porn in interpreting the distribution of non-consensual intimate content, regulating the distribution of non-consensual intimate content in Indonesian positive law and providing innovations in preventing and handling violence in the context of digital media in casu NCII. The results of the study show, First, the use of the term revenge porn is no longer relevant to be used in referring to the phenomenon of the distribution of non-consensual intimate content. Second, Indonesia already has special regulations regarding sexual violence regulated in Law No. 12 of 2022 concerning Criminal Acts of Sexual Violence (UU TPKS) which already includes KBGO. Third, the government's steps in preventing sexual violence in cyberspace are still minimal. Prevention efforts cannot be done only in terms of normative and educational provision, but also require technology-based innovation. The author tries to make a comparison with the UK and Meta Platform in terms of implementing face id-based technology.

INTRODUCTION

Background

The era of globalization has had a significant impact on the development of technology, one of which is information and communication technology which in turn produces various dynamics in human life. Advances in information and communication technology do facilitate social interactions that allow people to connect with each other easily and quickly. However, this progress also creates new space for the emergence of various forms of crime, where perpetrators use technology to carry out actions that harm others. One form of this crime is the distribution of electronic documents that have content that violates morality in the form of non-consensual intimate content or non-consensual dissemination of intimate images (NCII). This can be detrimental to others because

perpetrators usually use this intimate content to threaten or blackmail the party who is the object of the recording (victim) to comply with their wishes. This is a form of online gender-based violence (KBGO) which according to data from the National Commission on Violence Against Women (2019) most often attacks women with a percentage of 33% of 97 KBGO cases falling into the category of distributing photo or video content of someone's body without permission or NCII. NCII often occurs because of the encouragement of revenge factors as well as intimidation or blackmail. NCII triggered by revenge usually occurs in the context of a romantic relationship, especially when one party feels hurt due to a breakup, feels betrayed, or their wishes are not fulfilled so that the intimate content is used by one party as a tool to threaten the other party. This phenomenon is often referred to as revenge porn or revenge pornography.

Meanwhile, NCII triggered by factors outside of revenge motives, for example because they want to carry out blackmail, is called sextortion (sexual + extortion). It is called sextortion because there is sexual blackmail where extortion means blackmail and is carried out in the sexual realm. However, today, the use of these terms is no longer relevant because it is often associated as if the victim made the mistake first and deserves to be punished with threats so that it seems to show an attitude of blaming the victim (victim blaming).

Not only is the typology a problem, but also the increasing spread of sexual violence modes into the digital realm has clarified the existence of an imbalance of power in relations between men and women (imbalance power or power inequality. Male domination internalizes its dominant role in the form of sexual acts so that there is an inequality in relations between men and women. This is in line with the perspective given by Rosemary P. Tong in her book entitled 'Feminist Thought' which reveals that sexual practices are a form of male domination over women. PurpleCode Collective, a feminist community in Indonesia, also argues that the practice of sexual violence is more related to efforts to perpetuate domination and control over victims. The existence of this male domination actually results in sexual relations being used as a tool of oppression against women with the assumption that intimate relationships are something that is 'permitted' because of their natural nature.

In fact, Sexual Assault Prevention and Awareness has explained in its findings that consent is the most important aspect to determine whether an event can be categorized as sexual violence or not. Consent is given clearly, not ambiguously through words or actions towards an agreed activity. When giving consent, it must also be free from any influence or pressure so that the giver must be willing and in a free state to decide whether to agree or not. The concept of consent is the embodiment of the right to personal sovereignty. However, in reality, the concept of consent distorts the theory of male domination in sexual relations. The author argues that it is impossible for consent to be free from influences beyond the will of women.

This is an implication of hegemonic masculinity which allows consent to be given without physical coercion, but the impetus for consent comes from male dominance that is internalized in a relationship. Therefore, consent only changes harassment/rape into sexual liberation which actually normalizes male aggression for the justification of giving permission. This paradigm causes violence in sexual relations to be considered 'normal' as a form of male control in its superiority. Male domination results in sexual objectification of women which ultimately leads to gender oppression. The synthesis of male domination as male dominance and female subordination ultimately becomes a driving factor for various forms of sexual violence. Such as the practice of pornography, prostitution, rape, harassment, and sexual violence. In addition to the male domination theory, there is another theory that also shows that there is an imbalance in social, economic, and political power between women and men, which in turn strengthens male dominance. This theory is known as the traditional gender roles theory.

These two theories are causally related to each other which empirically explains that there is a causal relationship between the inequality experienced by women and men and male dominance itself, where the existence of inequality experienced by women gives birth to male dominance. As a result, women are the most vulnerable to sexual violence. Moreover, the development of forms of sexual violence has expanded after human life entered the digital era. The transition of conventional activities has dragged various forms

of crime that have expanded into digital spaces. This has also encouraged the birth of new forms of sexual violence that occur electronically. The presence of digital technology indirectly facilitates the occurrence of crimes against gender or what is called Technology Facilitated Gender Based Violence. The following phenomenon then developed and is known in various academic studies as Online Gender Based Violence ("KBGO").

Based on the explanation above, it appears that the presence of technology seems to add a new dimension to crime so that it not only brings different challenges, but also requires a more intensive handling approach adjusted to its unique characteristics. It is said to be unique because there are many ways to commit crimes with sophisticated technology. To overcome this challenge, comprehensive and sustainable prevention and handling efforts are needed by involving three instruments, namely legal and technological instruments as preventive efforts and psychological instruments as repressive efforts. Therefore, the author is interested in conducting research by examining: First, the dynamics of the typology of sexual violence and its regulations in positive law in Indonesia; Second, the concept of strict liability as a form of criminal responsibility for perpetrators as well as a replacement for the concept of responsibility that has been regulated in the TPKS Law; and Third, preventive and repressive efforts in dealing with KBGO by making comparisons from Australia through optimizing technology in the form of the stopncii.org website.

This research is inseparable from previous studies that have discussed similar topics, such as the writing compiled by Elika Angie Runtu entitled "Law Enforcement in Providing Protection for Women Victims of Crime Threats (Revenge Porn) that occurs on Social Media". The writing discusses the factors that increase revenge porn cases and prevention efforts along with legal efforts that can be taken for women victims of revenge porn. The writing also uses the term NCII to refer to revenge porn which the Author is then interested in discussing further through this writing.

However, this article is different from the one that will review the evaluation of the term revenge porn which is considered less relevant in the present era and the efforts that can be made both in terms of handling and preventing KBGO. In terms of prevention, the author offers the application of technological instruments by involving cross-sectoral cooperation.

Issue Formulation

1. How is the relevance of the Use of the Term Revenge Porn in interpreting the Spread of Non-Consensual Intimate Content or non-consensual dissemination of intimate images (NCII)?
2. How is the innovation of preventing and handling violence in the context of digital media?

Research Methods

The form of research applied by the author in this study is normative research, with the following approaches:

1. Conceptual approach, which in this study makes the concepts of thinking about the Spread of Non-Consensual Intimate Content or non-consensual dissemination of intimate images (NCII), male domination theory, hegemony masculinity theory, and strict liability theory as the main analytical tools in analyzing the issues in this study;
2. Statute approach, which in this study uses Law Number 12 of 2022 concerning Criminal Acts of Sexual Violence, Law Number 44 of 2008 concerning Pornography, and Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 5 of 2020 concerning Private Electronic System Organizers as analytical tools in analyzing the problem objects in this study; and
3. Comparative approach, which in this study, the author uses the practice of preventing and overcoming the Spread of Non-Consensual Intimate Content or non-consensual dissemination of intimate images (NCII) in Australia as a comparative instrument in analyzing the issues in this study.

Research Results

A. Relevance of the Use of the Term Revenge Porn in Understanding the Spread of Non-Consensual Intimate Content or non-consensual dissemination of intimate images (NCII)

Revenge Porn is often interpreted as revenge pornography because of the diction attached to it, namely revenge which when translated means revenge and porn which means pornography. However, in Indonesian positive law, the nomenclature of revenge pornography or revenge itself is not used in the elements of the crime, but is described as the distribution of sexual content without the right and without the consent of the related party. So it becomes interesting when this revenge porn is portrayed from a sociological perspective as an act of revenge, but is portrayed from a legal perspective as an act of distributing sexual content outside the will or without the consent of the person who is the object of the recording without requiring revenge.

The reason is, this will have implications for the evidence process in court. When the element of revenge becomes an element of the crime *(bestanddelen delict)* or is written *expressive verbis* (clearly and clearly) in the wording of the article, it means that revenge becomes the main requirement or in other words it must be proven by the Public Prosecutor that the perpetrator really has a motive for revenge behind the act of distributing sexual videos that he did. The next question is, what if there is a perpetrator who intentionally distributes a video containing sexual content without the consent of the person who is the object of the recording, but the goal is not for revenge? This is what should be the focus of attention to boost the paradigm of "revenge porn" that in reality revenge porn does not necessarily make revenge the main requirement.

B. Regulations Concerning KBGO in Indonesian Positive Law

The phenomenon of KBGO has a more destructive impact compared to conventional types of sexual violence. It does not mean that conventional types of sexual violence do not need to be considered, but KBGO also brings together other forms of crime, namely cybercrime. The massive destructive effect is a result of the speed and breadth of reach on the internet network. The following destructive effects not only affect the psychology of the victim but are almost comprehensive in various aspects such as the victim's mobility space, to the victim's economic situation due to digital traces that are difficult to erase. The author wants to show that the form of protection for KBGO victims is an urgency for the protection of human rights that need to be guaranteed. So, entering the third discussion, legally, as in article 12 of the Universal Declaration of Human Rights, which formulates

> *"No one shall be subjected arbitrarily with his privacy, family, home or correspondence, nor to attack upon his honour and reputation. Everyone has the right to the protection of the law against such,interference or attack"*

The following provisions are the foundation for the implementation of global human rights protection. The formulation of Article 12 has bound every country to provide a guarantee that no one can be treated arbitrarily against their privacy. Honor and reputation. The guarantee in question is implemented in the form of protection outlined in a legal instrument. In Indonesia itself, as regulated in the constitutional mandate in Article 28G Paragraph (1) of the 1945 Constitution of the Republic of Indonesia, it has provided a basis for the right for everyone to receive protection from all forms of threats to do or not do something. Therefore, the freedom in question can be contextualized as an individual's will regarding something about themselves. Departing from this, it shows the importance of guaranteeing legal protection for victims of sexual violence. The form of protection in question must be formulated by understanding a series of characteristics of the development of electronic-based sexual violence.

At the juridical-normative level, the State of Indonesia has had a number of regulations at the level of Laws that contain provisions regarding electronic-based sexual violence crimes. The legal instruments in question include Law No. 44 of 2008 concerning Pornography ("Pornography Law), Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions ("ITE Law"), and Law No. 12 of 2022 concerning Criminal Acts of Sexual Violence ("TPKS Law").

The elements formulated in Article 4 paragraph (1) of the Pornography Law include:

1. Everyone
2. Is prohibited from producing, making, reproducing, duplicating, distributing, broadcasting, importing, exporting, offering, trading, renting, or providing pornography;
3. Which explicitly contains;
4. Intercourse, including deviant intercourse, sexual violence, masturbation or onani, nudity or displays that give the impression of nudity, genitals, or child pornography.

Meanwhile, in the ITE Law, it is specifically formulated in Article 27 paragraph 1 of Law No. 11 of 2008, the elements of which include:

1. Any person
2. Intentionally and without right
3. Distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents
4. Which have content that violates morality

In addition to the ITE Law and the Pornography Law, Article 14 paragraph (1) of the TPKS Law also formulates elements of similar acts which include:

1. Any person
2. Who without right
3. Records and/or takes pictures or screenshots containing sexual content outside the will or without the consent of the person who is the object of the recording or picture or screenshot
4. Is punished for committing electronic-based sexual violence

Furthermore, Article 14 paragraph (2) of the TPKS Law also criminalizes acts as stipulated in Article 14 paragraph (1) of the TPKS Law if the act is carried out with the intention of blackmailing or threatening, coercing; or misleading and/or deceiving someone.

In the National Criminal Code, criminal acts related to pornography are regulated in Article 411 paragraph (1) with the following article formulation:

1. Any person
2. Who produces, makes, reproduces, duplicates, distributes, broadcasts, imports, exports, offers, sells, rents, or provides pornography.

From this explanation, a conclusion is drawn that the act of distributing intimate videos, whatever the motive (revenge and/or non-revenge, such as blackmail), as long as it is not for personal gain (based on the Explanation of Article 4 paragraph (1), then the act can be criminalized. The application of the article does not need to look at the "mens rea", but rather at the "actus reus" so that claims of a typology of revenge porn being wrong do not need to be questioned because the act of distributing sexual videos is something that has been criminalized regardless of any motive. The differences between the three legal instruments can be analyzed through the following table:

Perbandingan Undang-Undang yang berkaitan dengan muatan materi *Non Consensual Dissemination of Intimate Images*			
	Undang-Undang No. 44 Tahun 2008 tentang Pornografi	**Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik**	**Undang-Undang No. 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual**
Rumusan Pasal	**Pasal 4** Larangan dalam memproduksi, mendistribusikan dan memperjualbelikan konten bermuatan **pornografi** diantaranya memuat Persenggamaan, Kekerasan seksual. Masturbasi dan ketelanjangan **Pasal 6** Larangan untuk memperdengarkan, mempertontonkan, memanfaatkan, memiliki, atau menyimpan produk **pornografi** **Pasal 9** larangan menjadikan orang lain sebagai objek atau model, yang mengandung muatan **pornografi**	**Pasal 27 (1)** Larangan menyebarkan muatan informasi yang melanggar **kesusilaan**. Pasal 27 A **setelah perubahan kedua UU ITE) Larangan **menyerang kehormatan** atau nama Baik orang lain agar diketahui umum **Pasal 27B (1)** **setelah perubahan kedua UU ITE Larangan **menyebarkan informasi untuk menguntungkan diri** sendiri atau orang lain secara melawan hukum dengan memberikan ancaman kekerasan sebagai bentuk pemaksaan **Pasal 27B** **setelah perubahan kedua Larangan menyebarkan informasi untuk menguntungkan diri atau orang lain secara melawan hukum dengan ancaman pencemaran atau ancaman membuka rahasia, dengan memaksa orang memberikan barang yang sebagian atau seluruhnya milik orang tersebut atau orang lain	**Pasal 4 (1)** kategorisasi kekerasan seksual dalam 10 (sepuluh) bentuk. Pasa butir (i) eksplisit menyebut kekerasan seksual berbasis elektronik **Pasal 14 (1)** Tiga bentuk perbuatan yang termasuk dalam pidana kekerasan seksual berbasis elektronik 1. Melakukan perekaman atau mengambil gambar yang bermuatan seksual diluar kehendak objek yang di reka, 2. Mentransmisikan informasi elektronik yang bermuatan seksual di kuat kehendak pemerinerima yang ditujukan 3. Melakukan penguntitan atau pelacakan menggunakan sistem elektronik terhadap orang yang menjadi objek
Ruang lingkup pengaturannya	Segala suatu hal yang berkaitan dengan tindakan pornografi — pornografi yang dimaksudkan memuat adegan seksual sebagaimana pada klasifikasi yang disebutkan pada pasal 4	Segala sesuatu hal yang dianggap melanggar kesusilaan, dan hak privasi seseorang — pelanggaran yang dimaksud terjadi pada ruang media elektronik	
Masalah hukum	Ketentuan pasal 4 dan 6 Undang-Undang Pornografi berpotensi tumpang tindih dengan ketentuan dalam UU TPKS.	ketentuan pasal 27 (1) UU ITE mengenai frasa 'melanggar kesusilaan' menjadi bermasalah karena menggeneralisir bentuk delik kesusilaan sebagaimana bab XIV KUHP tentang melanggar kesusilaan. Sehingga korban menjadi berpotensi mengalami kriminalisasi akibat pasal berikut. UU ITE belum perspektif gender yang memadai	

Tabel 1. Perbandingan UU Pornografi, UU ITE, dan UU TPKS

Based on the 3 (three) legal instruments, the presence of the TPKS Law as the main legal umbrella in handling sexual violence is a breath of fresh air for the protection of victims of sexual violence in Indonesia. However, in its development, the TPKS Law is still limited in accommodating the development of forms of sexual violence in cyberspace. As in the academic manuscript of the TPKS Law, it has analyzed incidents of electronic-based sexual violence. In certain situations, it is possible for the victim to be willing to have sexual intercourse but is not willing

or aware that their activities are being recorded by the victim and are about to be exploited. However, in some of its developments, it is possible for the recording incident that occurs in electronic-based sexual violence to be carried out with the victim's consent.

As in the revengeporn case in 2018 which ensnared X, a student as a perpetrator of electronic-based sexual violence. During their relationship, it was known that X often asked his ex-lover to send intimate photos or videos. When associated with the concept of consent, the victim is willing to record and send sexual content to the perpetrator to be accessed and stored.

> *"Does this mean that X's ex-lover can be categorized as a perpetrator under the provisions of Article 27 of the ITE Law?"*

This should not happen, because the victim's conception must be kept away from the paradigm as the guilty party. In addition, the consent to the recording by the victim is a turning point for attaching blame to the victim's actions. However, if the red line with the male domination conception allows the victim to agree to the perpetrator's request even without physical coercion. So in this case, criminalization of victims of electronic-based sexual violence is something that is avoided. However, the legal consequences given in Article 27 of the ITE Law do not provide an adequate explanation of the meaning of the phrase "violating morality." This article opens up a big gap for victims of revenge porn to be criminalized. As if the victim had 'made' and 'distributed' a video with sexual content as something that was interpreted as violating morality as formulated in Article 27 of the ITE Law.

Apart from the ITE Law, the inharmonization of regulations that occurred in the Pornography Law also opened up a wide gap for victims of revenge porn to be suspected or even determined as perpetrators. Article 6 and Article 4 of the Pornography Law prohibit the act of producing, distributing, listening to, watching, and storing sexual content as the elements mentioned in Article 1 of the Pornography Law. As a result, the meeting point of the conceptual line of pornography with revenge porn becomes blurred. However, it should be emphasized that revenge porn is not part of pornography. In line with the opinion of Mcglynn (2018) that sexual activity in intimate relationships is not pornography. This is because the problem point in revenge porn is the type of sexual violence intended as NCII.

This means that the act that is prohibited by law is the act of spreading sexual content carried out by the perpetrator without the victim's consent. A number of actual cases have found a development model for revenge porn. This development is a form of commercialization carried out by the perpetrator by sending videos/photos of the victim to a paid pornography site. This means that the perpetrator's motive is no longer limited to revenge against the victim, but also exploits sexual content and makes a profit. So this blurs the definition of revenge porn with pornography, which allows victims of electronic-based sexual violence to be charged with articles in the Pornography Law and the ITE Law. Therefore, the law that regulates the distribution of sexually charged content must be directed to only be able to take legal action against the perpetrators. The perpetrators in question are anyone who distributes sexually charged content as a form of NCII crime.

The author wants to compare the intent of the statement above with Law No. 21 of 2007 concerning the Eradication of the Crime of Human Trafficking ("UU TPPO"). The TPPO Law in one of its material contents regulates the practice of prostitution or prostitution, by viewing it as a form of sexual exploitation. The legal paradigm used by the TPPO Law only takes legal action against acts committed by pimps as perpetrators of sexual slavery crimes. The TPPO Law does not consider prostitutes as perpetrators of prostitution crimes, but considers them as victims of sexual slavery. Therefore, to avoid criminalization of victims in revenge porn cases, it must also be ensured that it only targets perpetrators of sexual content distribution.

Based on this analysis, it can be seen that the TPKS Law has actually become a legal reform. The TPKS Law has harmonized the provisions of previous laws that still positioned victims as perpetrators of pornography or violating morality. This is done through the provisions in Article 14 Paragraph (4) of the TPKS Law, by excluding acts of recording, taking pictures or screenshots, and transmitting sexual content if done on the basis of self-

defense. Thus, victims of revenge porn cannot be punished with the validity of the following article, because they are considered to be defending themselves from acts of sexual violence. However, the TPKS Law is still limited in terms of the dimensions of handling and recovery for victims of sexual violence electronically. Based on research conducted by the Support Group and Resource Center on Sexuality Study ("SGRC"), handling revenge porn requires special handling because it is also related to cyber technology. The locus of revenge porn crimes does occur in the immaterial world (digital world) but its impact is still felt in the material world (real world). So cyber-based sexual crimes are a form of blurring the boundaries between the material and immaterial worlds.

This is because revenge porn brings causes from the immaterial world so that it produces effects in the material world. Handling of electronic-based sexual violence must be constructed progressively. Therefore, its handling requires a technical technological solution related to the removal of digital traces that have been carried out by the perpetrator. The author argues that the removal/takedown of the victim's sexual content is a unity that needs to be resolved together with the legal handling process. This has actually been regulated in Article 26 (4) of the ITE Law concerning the procedure for determining the court that can request the electronic system organizer to remove all information. However, the existence of the following article is half-hearted because it does not provide any legal consequences if it turns out that the electronic system organizer does not delete the related information.

The TPKS law regime has actually realized the importance of stopping the spread of sexual violence content in unlimited digital space. As in Article 46 of the TPKS Law, the central government has the authority to delete and decide on the existence of information or electronic documents containing criminal acts of sexual violence. However, the provisions regarding the following are only regulated in 1 (one) article so that its validity requires further provisions on who has the right to delete, what are the stages and processes of deletion, and what is the basis for the government to delete it. This shows that there is an urgent legal vacuum by holding a regulatory instrument at the government regulation level as soon as possible. The instrument must be considered in terms of the scope of its regulation so that it can be applied effectively. Therefore, the author formulates the following solution.

C. Innovation in Prevention and Handling of Violence in the Context of Digital Media

The rapid development of technology and its increasingly dominant role in human life are in line with the increasingly diversified modus operandi in carrying out violence in digital media. There are various methods that are usually used by perpetrators of KBGO in casu NCII, starting from using social media platforms, such as Instagram, Youtube, and Facebook, to web pages, such as dark websites and illegal website domains that are not registered with the Government so that it is easy for them to spread non-consensual intimate content because these pages are far from the reach of government regulations. Even though the government has regulated the provisions for the implementation of electronic systems and transactions properly in Article 95 and Article 96 of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, the regulatory domain of Article 95 and Article 96 is information/documents/electronic systems that have been registered with the government, while dark websites cannot be accessed in the usual way because their contents are not indexed by search engines.

Because the media used for crime is through technology, technological instruments are needed as an effort to prevent and handle the crime. This is in line with the theory of crime prevention, namely the Primary Prevention Theory which states that crime prevention can be done by changing the physical conditions of the environment that provide opportunities for crime to occur. In this case, cyberspace as a place that provides opportunities for NCII to occur, must be changed in such a way by involving technology as a cyber-based system to prevent NCII from occurring. This is a necessity for the government in efforts to prevent KBGO. Like in the UK, the local government is taking a technological approach to prevent the spread of non-consensual intimate content using the StopNCII.org platform. This platform was developed by involving the Revenge Porn Helpline in the UK. Through StopNCII.org., every individual who is a victim of the spread of non-consensual intimate content can proactively report evidence of the spread to institutions that have collaborated with StopNCII.org. Then the

victim will create a hash of their intimate content and create a digital fingerprint that can be used by StopNCII.org to detect and block intimate content to prevent further spread.

The way this platform works is called hashing technology where each video can be given a unique code through an encryption method. Prevention can be done by blocking or cutting off access to intimate content that has the same unique code content. However, the working system of this platform has a drawback because it will work effectively if the content is also owned by the victim. In the case where the content is only owned by the perpetrator, for example because they have recorded it secretly, it will be difficult for the victim to take preventive action, although after the video is spread, repressive efforts can still be made using hash technology as described in the previous paragraph. In addition to being able to work repressively, this hash technology is able to work at a preventive but limited level, namely when the victim also has the intimate document. The implication is that the victim can take early preventive action by providing a hash to the video before there is any threat or distribution from other parties.

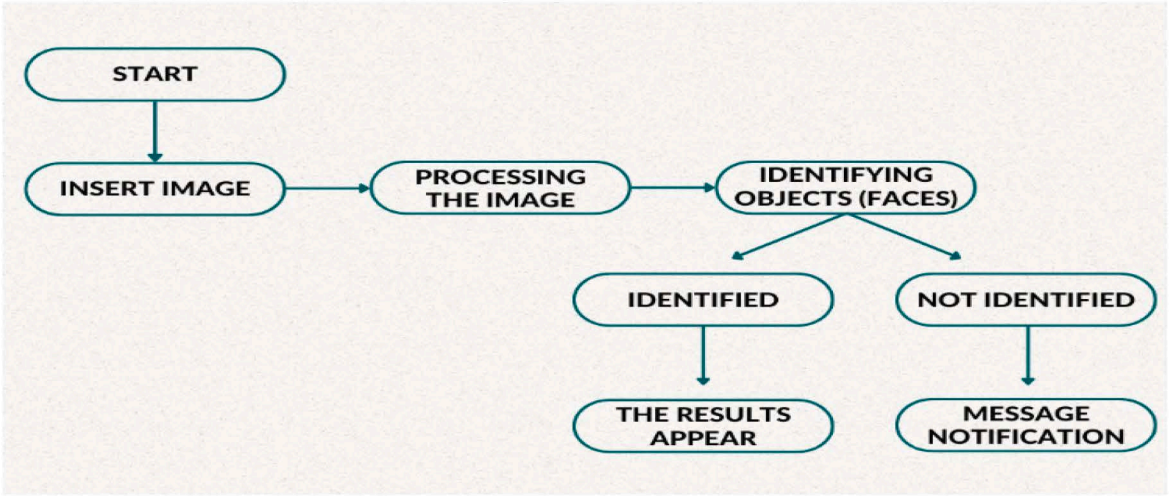
Based on the explanation above, the author wants to adopt this mechanism so that it can be applied in Indonesia in the following ways:

1. Forming a Cyber Protection Unit for Women as an implementing agency under the National Commission on Violence Against Women which coordinates with related elements that focus on receiving reports and handling Cyber in cases of sexual violence.
2. Creating cooperation between the Cyber Protection Unit for Women and StopNCII based in the United States in terms of transferring knowledge and technology for digital fingerprints or hashes used by StopNCII to identify intimate documents.
3. After transferring knowledge and technology with StopNCII, the Cyber Protection Unit for Women conducted a trial of implementing the hash through a technology called CyberShield, a platform that functions to prevent the potential spread of sexual content with a locking method through a unique code so that there is a block in the upload process on content with the same unique code.
4. After the trial is successful, the Cyber Protection Unit for Women will coordinate with the Ministry of Communication and Information to appeal to electronic system organizers to cooperate with the Cyber Protection Unit for Women to facilitate the sending of hashes.

The mechanism explained above is a preventive measure to overcome the spread of intimate content on social media. However, this mechanism only accommodates and works effectively if the victim saves the intimate video. To address the weaknesses of this preventive mechanism, the Author offers two solutions, namely the first solution which is normative and the second solution which uses technological instruments. The first normative solution refers to Article 11 of the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 5 of 2020 concerning Private Electronic System Organizers. Based on this regulation, the Cyber Protection Unit for Women through the Ministry of Communication and Information can order electronic system organizers to terminate take down access to content that has prohibited content or is not in accordance with applicable laws and regulations in Indonesia.

As for the second solution, the Author offers a face id-based technology solution. The Author realizes that the media that is often used to spread intimate content is through social media and websites. Social media operating in Indonesia is controlled by the Meta Platform company which houses social media applications, such as Instagram, Facebook, WhatsApp, Messenger, and others. Jerome Pesenti, vice president of artificial intelligence at Meta, once explained that facial recognition technology can be very useful in everyday life, even if it is only to unlock a cellphone. However, on the other hand, there are concerns about the lack of clear laws and limitations in using facial recognition technology. These concerns ultimately prompted META to close its facial recognition feature in 2021. At that time, this feature worked by identifying faces in a photo so that it was easier for users to tag other users in the image. However, it turned out that many users felt uncomfortable with the system regarding their privacy so this feature was disabled.

However, after the facial recognition feature was disabled, Meta spokesperson Jason Grosse said that facial recognition technology is an approach that will continue to be explored while considering how Meta's future computing platforms and devices can better meet the needs of the community. This means that public protests regarding facial recognition technology because it is considered to violate privacy are not the end of everything. The proof is that until now Meta continues to approach facial recognition technology while still considering the development of computing devices so that they can better adapt to the needs of the community. The facial recognition technology currently being developed by Meta is the Deepface Algorithm which works in the following way:



The development of the algorithm technology has been carried out by Facebook by acquiring face.com which is able to detect faces with a percentage of 97.25%. In line with meta's efforts to develop the technology, Indonesia can form regulations related to the use of facial recognition features for applications and their limitations so that the privacy of the Indonesian people is not disturbed. Efforts to form this regulation can be a safe space for meta to be able to apply its facial recognition technology in Indonesia without having to worry about legal vacuums. Moreover, this initiative is relevant to efforts to prevent NCII on social media which is a hotbed for the spread of non-consensual intimate videos so that the Author encourages the Meta Company to re-implement the facial recognition feature with a new scheme. Facial recognition is no longer in the form of photo tags, but in the form of a security scheme to protect other users whose privacy rights are violated.

Technically, how this technology can help prevent the spread of intimate videos that have the potential to violate the privacy of others will be elaborated as follows:

1. A (woman) and B (man) are a couple who have had a relationship like husband and wife.
2. One time their relationship was strained. Based on his annoyance with A, B deliberately spread the intimate video that he had secretly recorded to his Instagram account.
3. The Instagram application already has a face id feature by utilizing the deepface algorithm which can function as a filter to filter the security of content before it is uploaded.
4. In carrying out its function as a filter, this algorithm works by identifying objects in the content. Objects are not only limited to faces, but also include elements or patterns that indicate elements of nudity.
5. If the element of nudity is identified, the algorithm will record the face in the content and delay the upload. When the upload process occurs, the deepface algorithm stops working.
6. When the deepface algorithm stops working, AI that works with the help of machine learning so that it can collect all information can identify the owner of the face.
7. After the owner of the face is identified, AI will work by sending a notification to the device of the owner of the face to request verification and approval of the upload. The owner of the face identified in the element of nudity can verify that the object is indeed him and reject the upload.

Based on this explanation, there are two technological instruments that work complementary here; First, the deepface algorithm that is tasked with identifying objects, not limited to faces, but identifying content that violates the provisions of the law in Indonesia (this needs to be done because meta companies that want to open their markets in Indonesia must comply with the rules in Indonesia); and second is AI that works with machine learning so that it can recognize the owner of the face by sending a notification to the owner's device. If the owner is not an Instagram user, the notification can be sent via email or short message. This is the technology that we plan to apply in Indonesia under the name CyberShield.

Conclusion

The urgency of handling cyber-based sexual violence requires real action in an effort to stop the spread of sexual content in digital space. The long-term effects of cyber-based sexual violence leave long-term digital traces. As a result, it will erode the victim's psychology continuously. Significant losses continue to haunt victims due to shame and trauma from the content that is still available in digital media space. This indicates the destructive effect and the magnitude of the losses experienced by victims, indicating that the handling of sexual violence a quo, especially cyber-based sexual violence, has not produced anything. Victims will continue to be haunted by prolonged fear due to the downstream problems experienced by victims not being guaranteed to be resolved even in court. This means that the content of sexual content that continues to be stored forever in digital media will ultimately have a lasting impact throughout the victim's life. Therefore, this handling needs to be carried out progressively, not only using legal instruments, but also technological instruments whose management is under an institution that has the authority to terminate access to the victim's sexual content.

Daftar Pustaka

Peraturan Perundang-Undangan

Undang-Undang Tentang Pornografi, UU Nomor 44 Tahun 2008. LN Tahun 2008 No. 181 TLN No. 4928.

Undang-Undang tentang Perubahan Kedua Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 1 Tahun 2024 LN Tahun 2024 No. 1, TLN No. 6905.

Undang-Undang Tentang Tindak Pidana Kekerasan Seksual, UU Nomor 12 Tahun 2022. LN Tahun 2022 No. 120 TLN No. 4928.

Undang-Undang Tentang Pemberantasan Tindak Pidana Perdagangan Orang, UU Nomor 21 Tahun 2007. LN Tahun 2007 No. 58 TLN No. 4720.

Skripsi

Azzahra, Hajar Nabila. (2019). *Studi Pelaku Revenge Porn Sebagai Bentuk Kekerasan Seksual Terhadap Perempuan Berbasis Siber (Studi Kasus TH, RB, dan LM Pelaku Revenge Porn).* (Skripsi Sarjana Universitas Indonesia).

Puteranda, Rizky Hanif. (2020) *Objektifikasi Perempuan, Komodifikasi dan Social Capital dalam Revengeporn di Indonesia*. Makalah disajikan oleh Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Indonesia.

Jurnal Artikel

Sugiyanto, Okamaisya. (2021). Perempuan dan Revengeporn: Konstruksi Sosial Terhadap Perempuan Indonesia dari Perspektif Viktimologi." *Jurnal Wanita dan Keluarga.* Vol. 2. No. 1 Hlm. 23-29.

Faizah, Azza Fitrahul., & Hariri, Muhammad Rifai Hariri. Pelindunan Hukum terhadap Korban *Revenge Porn* Sebagai Bentuk Kekerasan Berbasis Gender *Online* Ditinjau dari Undang-Undang No. 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual. *Jurnal Hukum Lex Generalis.* Vol. 3. No. 7 Hlm. 520-532.

Brown, Jonathan. (2018). Revenge Porn and The Actio Iniuriarum: Using 'Old Law' to Solve New Problems.

Jurnal Legal Studies. Hlm. 1-15.

Khoirunisa, Dela. (2022). "Pelecehan Seksual Melalui Media Sosial Ditinjau dari Pasal 27 Ayat (1) Undang-Undang Tentang Informasi Transaksi Elektronik. *Jurnal Lex Renaissance.* Vol. 2. No. 7. Hlm 371-382.

Ma'sumah, Mufidatul., & Salmah, Halimatus Khalidawati, & Oktovani, Bellinda. (2024). Perlindungan Hukum Terhadap Perempuan Korban *Revenge Porn* yang Dibuat Berdasarkan Kesepakatan *(Based on Consent.) Jurnal Bedah Hukum.* Vol. 8, No. 1. Hlm. 229-241.

Sinaga, Debora., & Lidya, Ivana. (2024), Perlindungan Hukum dan Pertanggungjawaban Tindak Pidana Revenge Porn Berdasarkan UU No. 11 Tahun 2008 tentang Informasi Transaksi Elektronik (ITE) dan UU No. 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (TPKS). *Jurnal Padjadjaran Law Review.* Vol. 12. No. 1 . Hlm. 32-43.