

**JURIDICAL ANALYSIS OF THE USE OF ARTIFICIAL INTELLIGENCE IN HANDLING  
THE CRIME OF SEXUAL HARASSMENT IN CYBERSPACE****Efi Nurnaningsih**Law Department, Faculty of Law and Economics, Universitas Muhammadiyah Bima  
[nurnaningsiherfinda@gmail.com](mailto:nurnaningsiherfinda@gmail.com)**Taufik Firmanto**

Law Department, Faculty of Law and Economics, Universitas Muhammadiyah Bima

**Ridwan**

Law Department, Faculty of Law and Economics, Universitas Muhammadiyah Bima

**Syamsuddin**

Law Department, Faculty of Law and Economics, Universitas Muhammadiyah Bima

**Aman Ma'arij**

Law Department, Faculty of Law and Economics, Universitas Muhammadiyah Bima

**M. Farizan Islam**

Law Department, Faculty of Law and Economics, Universitas Muhammadiyah Bima

**ABSTRACT**

The increase in information technology crime is increasingly widespread, where people use this technology as a means to violate the law. Information technology has influenced and encouraged changes in the social and economic needs of society. This research focuses on how to preventively control sexual violence on social media. As well as the role of artificial intelligence in preventing some applications that are often misused by some parties to find victims who can be harassed, with the Electronic Information and Transaction Law in sexual violence. The method / approach used is the normative method by looking for literature journal articles, and relevant sources. The results of this study include.1. This harassment occurs due to a lack of sex education and a lack of morality from individuals so that they do things that violate the norms of decency and norms of decency, the lack of education from these individuals is the cause of sexually harassing behavior; 2. artificial intelligence that will search for content that smells of child sexual abuse on the internet. Google Content Safety API uses a network to scan photos by making images that are considered inappropriate less conspicuous; 3. Replacing and/or tracking using electronic systems against people who are objects in electronic information/documents for sexual purposes. This research is expected to be a solution in dealing with sexual violence on social media.

**Keywords:** Artificial Intelligence, Crime, Sexual Offenses.

## INTRODUCTION

Every individual today has a personal cell phone with various brands and models. Especially today, cell phones have become a common device held by everyone, wherever they are. Technological advancements have changed the social structure of society from local to global. For example, computers, which were originally only used as fast calculating machines, have now become tools capable of performing a variety of data processing tasks and play an important role in electronic data storage Purwani, D. A. (2021). This change is triggered by the development of information technology, which has impacted modern society by introducing new types of crime that did not exist before.

One of the consequences of the pervasive use of information technology is the growing prevalence of criminal activities facilitated by this technology. Individuals have increasingly turned to information technology as a means of circumventing the law. Information technology has exerted a profound influence on the social and economic landscape, prompting a transformation in the fundamental needs of society. The transition from conventional to electronic transactions and social interactions is driven by the perception that digital processes are more effective and efficient Ahmad, A., & Nurhidaya, N. (2020). However, rapid developments in internet technology have also given rise to new crimes such as provocation, money laundering, system hacking, software and hardware theft, and other crimes.

Internet crime, also known as cybercrime, is a form of crime that harms and worries society Ketaren, E. (2016). These crimes often occur in the mass media and include any form of use of computer networks for high technology-based criminal and/or criminal purposes. One example is sexual harassment in the mass media, where the majority of victims are women Cut Salma, H. A. (2021). Sexual harassment in the mass media, both in the form of verbal and non-verbal harassment, has become a common occurrence and is no longer considered taboo.

Additionally, instances of sexual harassment have been publicized through television media, including advertisements for cigarettes, energy drinks, illicit substances, and contraceptives. These instances are directly related to the image and role of women. Such products frequently employ images of women for the sole purpose of attracting attention, utilizing stereotypes that dehumanize women and incite controversy related to sexual harassment Rafidati, T., Fitri, M. P., & Fadilla, S. A.

(2022). Nevertheless, the government's endeavors to confront this problem have been less efficacious due to its inability to respond in a commensurate manner to criminal techniques perpetrated through computer technology, particularly within the context of internet networks. The reporting of sexual harassment against women in the context of technology and information media is currently impeded by a number of factors. These include the tendency for victims to be subjected to greater stigma than perpetrators, questions that focus on the victim's attire and behavior, and the assumption that victims are attention-seeking or lying. In such circumstances, a considerable number of women and men who have been subjected to sexual harassment believe that disclosing their experiences is unwarranted.

The internet has facilitated human interaction and information search, eliminating time and space constraints through the internet network Sosiawan, E. A. (2020). However, the development of information technology also brings the possibility of the birth of new criminal acts, which occur through virtual media or the virtual world using technology as a tool. The term “cybercrime” is used to describe criminal activities that are conducted through the use of computers and cyberspace. These activities are referred to as “virtual media” or “virtual world” crimes. Cybercrime encompasses a multitude of illicit activities, including but not limited to hacking, carding, phishing, defacing, spamming, and the use of malware. The prevalence of malware in Indonesia is a significant cause for concern, as evidenced by data from Microsoft's cybersecurity division at the end of 2018. This data indicates that Indonesia is the third most affected country in terms of malware infections on computer devices.

A review of internal data from the company's cyber security center in Washington, USA, revealed that the most prevalent cyber-attack in Indonesia is malware. Malware remains a significant concern in the cyber domain due to its ability to evade detection for extended periods. This is achieved through the use of sophisticated techniques designed to remain undetected by the system owner, thereby circumventing the usual security measures. The current era of technological advancement is now entering an era defined by the advent of artificial intelligence (AI), a field of study that has gained significant traction in recent years. AI refers to the simulation of human intelligence by machines programmed to think humanly and mimic their actions, artificial intelligence itself is characterized by the ability to reason and take actions that have the best chance of achieving certain goals Fatmawati, F., & Raihana, R. (2023). The application of artificial intelligence (AI) represents a significant area of focus in the context of the Industrial Revolution 4.0, where the exploitation of Big

Data and AI represents a pivotal aspect of the revolution itself. Artificial intelligence (AI) is a technology that is being used in numerous business organizations around the world for the purpose of controlling company data. Furthermore, the use of machine learning to gain insight into business trends is becoming increasingly prevalent Rachmadie, D. T. (2020). But on the other hand hackers are also exploring this technology to create AI-powered malware that can spread untraceable malicious applications in harmless data payloads. AI techniques can hide the conditions required to open a malicious payload making it almost impossible to reverse engineer the threat, they also have the potential to bypass modern anti-virus and malware intrusion detection systems. AI-enabled malware can be trained to wait until a specific action occurs that triggers the hostile payload. This might be driven by voice or facial recognition, or even by geo-location properties. It can be said that AI malware can be trained to listen for specific words or the voice of the targeted person.

One of the difficult things that will be found in the legal handling of malware distribution crimes is when the legal process is constrained because the perpetrator cannot be found or there is no person / group that can be held accountable for the crime and usually the perpetrator comes from abroad Habibi, M. R., & Liviani, I. (2020). In Indonesia, there has not been a deepfake attack or other AI-malware mode, but malware attacks have been rampant and AI technology has now begun to develop, making us introspective about cyber security.

Law Number 11 of 2008 concerning Electronic Information and Transactions articles 27, 28, 45 (1, 2) explain about information technology crimes in the form of sexual crimes in the mass media with the aim of providing legal protection in the form of special protection instruments, in the enforcement of sexual harassment cases, there are several obstacles in terms of proving and solving cases to reveal crimes. Efforts made by the police in this case are constrained by legal awareness, according to psychologist and advocate for victims of sexual harassment, Beverly Engel, in her article on Psych Central, there are four reasons why there are many women who are reluctant to report their cases to the authorities due to the denial that they are victims of sexual harassment do not realize what someone is doing as sexual harassment due to ignorance, fear of consequences especially sometimes the victim knows the perpetrator of sexual harassment such as from family factors, especially if it is extreme sexual harassment that causes shame to the victim because things related to sexuality in our society are still taboo supported by the phenomenon of blaming victims who are mostly women still

occurs due to double standards of moral values, women are considered as figures who must maintain morals, behavior, and various other views.

## **METHODS**

Normative legal research encompasses an array of legal disciplines, including the examination of legal principles, legal systematics, the level of legal synchronization, legal history, and comparative law. In order to address the aforementioned issues, the author will undertake an examination of the fundamental principles and systematic structures that underpin the legal system. The objective of this research is to identify the legal rules that have been formulated within a given field (legal system) and to ascertain how these rules are applied.

## **RESULTS AND DISCUSSION**

### **Juridical Analysis Of The Use Of Artificial Intelligence**

The development of computers today responds to the changing times and what is happening with the world community who always want to find something new through processing, research and development and make new complex and modern discoveries from the results of their thinking Suisno, S. (2014). Artificial intelligence (henceforth referred to as AI) is the study of how to enable computers to perform tasks that are currently carried out more effectively by humans. The sheer number of complex problems currently faced by humans makes it challenging for humans and even computers to find solutions Santo Gitakarma, M., & Tjahyanti, L. P. A. S. (2022). Malware or Malicious Software is software that is explicitly designed to perform malicious activities or destroy other software Cahyanto, T. A., Wahanggara, V., & Ramadana, D. (2017). Both are the result of technological advancement. Artificial intelligence (AI), a product of technological innovation, has the potential to transform malware, which represents a significant challenge to technological security, into a formidable weapon. Malware-AI criminal acts have manifested in various forms, including the creation of deepfake videos or voice recordings, jackpotting, phishing spear-phishing, and numerous others.

By introducing a new invention of artificial intelligence that will search the internet for child sexual abuse content. The Google Content Safety API uses a network to scan photos by making

inappropriate images less conspicuous. Here's how Google's artificial intelligence works. This artificial intelligence is something that will be very useful in the future Pabubung, M. R. (2021). This is due to the prevalence of sexual harassment material on the internet, which is often left unmonitored and accessible to the general public. As reported by Google, this artificial intelligence has the potential to enhance the performance of reviewers by up to 700% compared to their previous capabilities. In light of the alarming increase in child sexual abuse, Google anticipates that this will contribute to further advancements in the fight against it.

“Crawler” is an effective program in preventing the spread of child sexual abuse content. However, this technology cannot record content that has not been marked as illegal Fachrurrazy, M., & Siliwadi, D. N. (2020). Consequently, manual monitoring by humans is still necessary to assess its autonomy. One of the primary organizations dedicated to the prevention of the dissemination of child sexual abuse material online is the Internet Watch Foundation (IWF), which collaborates closely with Google. Despite its UK headquarters, the group enjoys the support of major technology companies, including Google. It is anticipated that the advancement of Google's artificial intelligence technology will facilitate a more expedient cessation of the dissemination of sexually explicit content. This is a welcome development for many organizations engaged in addressing sexual harassment issues on a global scale. This will facilitate the processing of data pertinent to the issue of child sexual abuse.

#### Australian regulations for AI sexual harassment prevention

Australia has asked search companies such as Google and Bing to stop the spread of AI-produced child sexual abuse content. According to Reuters, e-Safety Commissioner Julie Inman Grant “we are asking search engine companies not to display child sexual abuse content on search engines.” The rules also prohibit the ability of search engine AI to create synthetic versions of the same content, she added. Deepfakes is another name for synthetic copies of this content. The issue of artificial intelligence-assisted child sexual abuse is being aggressively addressed by the attorneys general of all 50 states in the United States. Currently, many criminals are using AI technology to produce highly fake content or highly realistic fake photos Novyanti, H., & Astuti, P. (2021). In addition, although law enforcement aggressively investigates incidents of crimes against children online, crimes caused by AI are very difficult to prosecute. The physical, psychological, and emotional health of children who are victims of online sexual abuse, as well as the parents of those children, are severely jeopardized. The signatories of this letter encourage Congress to establish a

committee to find ways to address the risk of child sexual abuse posed by AI. Major social media platforms have implemented bans on this type of content, but there are still ways for it to spread.

### **Dealing With The Crime Of Sexual Harassment In Cyberspace**

The research results are explicitly summarized. The interpretation of the findings is done using logic and existing theories. Findings in the form of field, sociological, conceptual or normative realities are integrated with the results of previous research or with existing theories. For this purpose, there must be a reference. In generating new theories, old theories can be confirmed or rejected.

The term “harassment” is derived from the word “leceh”, which denotes disparaging or insulting conduct. In the context of English, the term “sexual harassment” is used to describe a specific form of misconduct. The word “harass” is defined as “to tease or annoy persistently,” which is often associated with creating a sense of anger or distress in the victim. In general, sexual harassment can be defined as any form of sexually attractive behavior that is unwanted and causes the victim to experience feelings of anger, distress, and so forth. Social media is regarded as an online platform that offers users the opportunity to engage with ease. Fitriani, Y. (2017). Social media in another opinion suggests as an online media platform intended by the community to interact that utilizes web-based technology in its interactions the use of social media that is not good or not based on the norms of decency and norms of decency by certain individuals often occurs and causes the emergence of deviant behavior such as sexual harassment. Sexual harassment can occur in several social media platforms, such as: “*Instagram, Facebook, Twitter, Whatsapp, Line, TikTok, and so on*”. The sexual harassment can be in the form of irresponsible comments or direct messages / personal messages such as mentioning the victim’s intimate parts, inviting the victim to have sex with the lure of providing payment, and so on that smell of sexual harassment Oktora, E., & Karli, K. (2023).

The harasser may be someone we know and consider it a “joke” in a friendship relationship but the person does not pay attention to the feelings of the victim with the words that the person says as a joke but follows or likes our social media account. Sexual harassment is referred to as unnatural and unwanted sexually attractive behavior, including invitations to sexual relations and other behaviors that refer to the act of sexual intercourse. Sexual harassment that often occurs consists of “20% verbal or intonation of voice that refers to harassment and 80% non-verbal”. Sexual harassment

is divided into two forms namely: “physical or non-verbal sexual harassment” and “non-physical or verbal sexual harassment”.

Non-verbal sexual harassment manifests as physical contact with the victim’s body, including groping, touching, or holding the victim’s limbs. Such actions are designed to humiliate and intimidate the victim. Verbal sexual harassment can be defined as any form of communication, whether spoken or written, that is directed at the victim with the intention of causing embarrassment and intimidation. An attitude of ignorance and acquiescence contributes to the rising prevalence of this deviant behavior in society Oktora, E., & Karli, K. (2023). Sexual harassment can be defined as a form of violence that is sexual in nature. It is characterized by the act of providing abnormal attention in a sexual manner, whether verbal or written, to an individual of the opposite or same sex, which is not desired by the victim. The scope of sexual harassment is vast and encompasses a multitude of forms, both verbal and written, physical and non-physical. These forms include, but are not limited to, verbal expressions such as inappropriate words or sexual jokes.

Sexual harassment in physical form can be in the form of poking, fingering, stroking, hugging, and so on. Acts of sexual harassment often occur and experience an increase every year but there is no separate regulation that is firm in regulating these acts. Mild sexual harassment such as sexually related verbal comments, jokes or whistles, and non-verbal in the form of facial expressions, body movements or other actions that request unwanted sexual attention that is harassing or insulting to the victim.

It is a criminal act, according to prevailing opinion, to engage in sexual harassment on social media. Criminal acts are defined as acts that are not permitted under the law and are subject to criminal penalties for those who engage in them. The prohibition is aimed at the act itself, while the sanctions are directed at the individuals who violate the prohibition. The protection of victims of sexual harassment is still lacking and the public’s view of victims of sexual harassment is often more judgmental towards their victims with inappropriate words. The community often blames and accuses the victim for being considered wearing clothing that is said to lead to a sexual harassment behavior or considers the victim’s behavior as the basis for the emergence of such behavior.

In the field of moral philosophy, it is posited that the foundation of criminal acts is immoral behavior that is subject to criminal punishment. Morality encompasses the concepts of virtuous and immoral human actions. The impact of immoral acts can be considered analogous to that of sexually

harassing behavior. This behavior causes the victim to experience harm in both physical and spiritual domains. Legislation in Indonesia, especially criminal law in regulating sexually harassing behavior through social media platforms, the resolution of these acts for now can only use several rules such as Article 281 paragraph (2) of the Criminal Code, Article 289 of the Criminal Code, Article 9 of the Pornography Law, Article 35 of the Pornography Law, and Article 27 paragraph (1) of the Electronic Information and Transaction Law, as follows:

Article 281(2) of the Criminal Code:

*“Any person who with deliberate intent and in front of another person who is there against his will violates decency”*

Article 289 of the Penal Code:

*“Any person who with violence forces someone to commit or tolerate obscene acts, shall, being guilty of an act offensive to the honor of decency, be punished by a maximum imprisonment of 9 years”*

Section 9 of Law No. 44 of 2008 on Pornography:

*“Every person is prohibited from making another person an object or model that contains pornographic content”*

Section 35 of Law No. 44 of 2008 on Pornography:

*“Any person who makes another person as an object or model containing pornographic content as referred to in Article 9 shall be punished with imprisonment for a minimum of 1 year and a maximum of 12 years and/or shall be fined a minimum of IDR.500,000,000 (five hundred million rupiah) and a maximum of Rp. 6,000,000,000 (six billion rupiah)”*.

Article 27 paragraph (1) of Law number 11 of 2008 concerning Electronic Information and Transactions:

*“Every person intentionally and without the right to distribute and/or transmit and/or make accessible Electronic Information and/or Electronic Documents that have content that violates decency”*.

The use of the Pornography Law as one of the bases for resolving criminal acts of sexually harassing behavior in social media because it is stated in Article 1 number 1 “Pornography is images, sketches, illustrations, photos, writings, sounds, sounds, moving images, animations, cartoons, conversations, gestures, or other forms of messages, through various communication media and / or performances in public, which create obscenity or sexual exploitation that violates the norms of

decency in society”. Sexually harassing behavior in sexual media includes the elements stipulated in the article, namely “writings, photographs, conversations, and messages that contain elements of obscenity and violate the norms of decency in society”. The Law on Pornography is said to be the “*lex specialis* (more specialized law)” of the Electronic Information and Transaction Law and the Criminal Code in terms of sexually harassing crimes through social media.

Sexually harassing behavior is one part of the offense of decency contained in Article 27 paragraph (1) of the Electronic Information and Transaction Law and the Criminal Code. The Law stipulates that “every person committing pornography does not regulate verbal harassment so it can be concluded that this Law can be applied when committing acts of verbal sexual harassment regulated in the Law”. The formulation in Article 27 paragraph (1) of the Electronic Information and Transaction Law states “that the object of the criminal act in the form of electronic information / documents, including in criminal acts in the field of information and electronic transactions, has a legal interest that needs to be protected, namely in terms of maintaining the values of decency that exist in the community”. Victims of criminal acts of sexual harassment in social media are regulated in Law No. 31 of 2014 concerning Witness and Victim Protection (UUPSK) “victims can and are legally entitled to protection and are free to choose what type of protection they want, are freed from all pressure to provide information, are protected from all types of questions that are tricky, guarantee compensation for losses, and are given legal advice.” [Ibid, p. 120].

Formulate specific rules related to sexually harassing behavior in social media in the Draft Law on the Elimination of Sexual Violence (RUUPKS). Specific rules on sexually harassing behavior in social media must be in the Draft Law on the Elimination of Sexual Violence, the Draft Law on the Elimination of Sexual Violence does not provide a more specific meaning of sexually harassing behavior but in article 11 paragraph (1) sexual harassment is included in the category of sexual violence [ Ibid, p. 120].

## CONCLUSION

Artificial intelligence is something that will be very useful in the future. That is because there is a big problem where things related to sexual harassment are often left on the internet and circulate freely without supervision. “Crawler” is an effective program in preventing the spread of content containing child sexual abuse. It should be noted, however, that this technology is unable to record

content that has not been flagged as illegal. Consequently, manual monitoring by humans is still required to assess its autonomy. One of the primary organizations dedicated to the prevention of the dissemination of child sexual abuse material online is the Internet Watch Foundation (IWF), which collaborates closely with Google. Despite its UK headquarters, the group enjoys the support of major technology companies, including Google. It is anticipated that the advancement of Google's artificial intelligence technology will facilitate the expeditious cessation of the dissemination of sexually explicit content. This is welcomed by many organizations dealing with sexual harassment issues around the world. Because it will make it easier to process data that will be related to the problem of sexual harassment. One of the interesting and feasible strategies to defend society from this huge threat is AI sexual harassment prevention. Have questions about virtual reality, augmented reality and other technologies

#### REFERENCES

1. Betty Yel, M., & M Nasution, M. K. (2022). Information Security of Personal Data on Social Media. *Journal of Kaputama Informatics (JIK)*, 6(1), 92-101.
2. Purwani, D. A. (2021). Digital era empowerment. *Bursa Ilmu*.
3. Ahmad, A., & Nurhidaya, N. (2020). Social media and the future challenges of the millennial generation. *Avant Garde*, 8(2), 134-148.
4. Ketaren, E. (2016). Cybercrime, cyber space, and cyber law. *Times Journal*, 5(2), 35-42.
5. Cut Salma, H. A. (2021). Framing Analysis of Sexual Violence News on Online Mass Media Serambinews. com 2020-2021 Period (Doctoral dissertation, UPT. Library).
6. Rafidati, T., Fitri, M. P., & Fadilla, S. A. (2022). Exploitation of Female Sensuality in Sukoka Candy Advertisement. *Journal of Audience*, 3(1), 61-71.
7. Sosiawan, E. A. (2020). The use of social networking sites as a medium of interaction and communication among students. *Journal of Communication Science*, 9(1), 60-75.
8. Fatmawati, F., & Raihana, R. (2023). Juridical Analysis of Artificial Intelligence in the Crime of Spreading Malware in Indonesia. *Innovative: Journal Of Social Science Research*, 3(2), 12190-12201.
9. Rachmadie, D. T. (2020). Regulation of Artificial Intelligence Deviation in Malware Crime Based on Law of the Republic of Indonesia Number 19 of 2016. *Recidive: Journal of Criminal*

- Law and Crime Prevention, 9(2), 128-156.
10. Habibi, M. R., & Liviani, I. (2020). Information Technology Crime (Cyber Crime) and Its Countermeasures in the Indonesian Legal System. *Al-Qanun: Journal of Islamic Legal Thought and Reform*, 23(2), 400-426.
  11. Suisno, S. (2014). THE CRIMINAL OFFENSE OF SPREADING VIRUSES ON THE INTERNET IN CONNECTION WITH THE INFORMATION TECHNOLOGY LAW. *Independent Journal*, 2(2), 51-59.
  12. Santo Gitakarma, M., & Tjahyanti, L. P. A. S. (2022). The Role of Internet of Things and Artificial Intelligence in Current Technology. *KOMTEKS*, 1(1).
  13. Cahyanto, T. A., Wahanggara, V., & Ramadana, D. (2017). Malware analysis and detection using dynamic analysis malware and static analysis malware methods. *JUSTINDO (Indonesian Journal of Information Systems and Technology)*, 2(1).
  14. Pabubung, M. R. (2021). Artificial Intelligence (AI) Epistemology and the Importance of Ethical Science in Interdisciplinary Education. *Indonesian Journal of Philosophy*, 4(2), 152-159.
  15. Fachrurrazy, M., & Siliwadi, D. N. (2020). Regulation and Supervision of Fintech in Indonesia: Sharia Economic Law Perspective. *Al-Syakhshiyah Journal of Islamic Family Law and Humanity*, 2(2), 154-171.
  16. Novyanti, H., & Astuti, P. (2021). Legal Snares for Misuse of the Deepfake Application in Review of Criminal Law. *Novum: Journal of Law*, 31-40.
  17. Fitriani, Y. (2017). Analysis of the utilization of various social media as a means of disseminating information for the community. *Paradigma*, 19(2), 148-152.
  18. Oktora, E., & Karli, K. (2023). JURIDICAL ANALYSIS OF WOMEN AS VICTIMS OF SEXUAL HARASSMENT IN MASS MEDIA. *Publika Scientific Journal*, 11(1), 116-121.
  19. Pratami, D.W. (2020). COMPARATIVE LAW OF VERBAL SEXUAL HARASSMENT THROUGH SOCIAL MEDIA IN INDONESIA AND THE PHILIPPINES AS AN ELEMENT OF VIOLATION OF DECENCY.