Locus: Jurnal Konsep Ilmu Hukum
E-ISSN: 2809-9265
Volume 6, Number 1, March 2026

A Juridical Analysis of Artificial Intelligence Misuse for the Sexual Exploitation of Women's Photo on Platform X Under Indonesia Positive Law

[1.*] Rhesas Shalatan
[2.] Mega Fitri Hertini

[1.2.] Faculty of law, Tanjungpura University, Indonesia.
[*.] Corresponding author, email: a1011241261@student.untan.ac.id

https://doi.org/10.56128/jkih.v6i1.875

ABSTRACT: This article aims to analyze the misuse of Artificial Intelligence (AI) on platform X for the sexual exploitation of women's photos and assess the effectiveness of Indonesian positive law in providing protection. This article applies a juridical-normative method through a statute approach to examine regulations related to the misuse of AI. The results of the study indicate that positive legal frameworks such as the 1945 Constitution, the Criminal Code, the Pornography Law, the ITE Law, the PDP Law, and the TPKS Law can be used to address the misuse of AI for sexually suggestive photo manipulation. However, all of these regulations do not specifically and explicitly regulate AI-based technology crimes, so law enforcement still relies on broadening the interpretation of the offense. Therefore, there is a need for more specific and adaptive regulatory updates to AI developments and increased responsibility of digital platforms in preventing the misuse of AI-based technology.

KEYWORDS: Abuse, Artificial intelligence, Platform X, Sexual Exploitation.

INTRODUCTION

Today, as Generation Z, who have grown up in a rapidly developing digital environment with open access to the internet, technological developments, and information, can bring about changes that influence mindsets and lifestyles. In this day and age, the need for the internet, communication tools, and various social media platforms has become an integral part of everyday life. The social identity, communication methods, and self-discovery process of this generation take place in a dynamic and open digital space. Familiarity with this technology means that Generation Z no longer sees the virtual space as an alternative reality, but as an integral part of social life. This situation has given rise to visual, fast, and responsive patterns of interaction that may open up opportunities for new forms of crime that were previously unknown to previous generations (Shalatan et al., 2026).

In the past five years, the pace of technological development has accelerated significantly. Various activities that were previously carried out conventionally have now

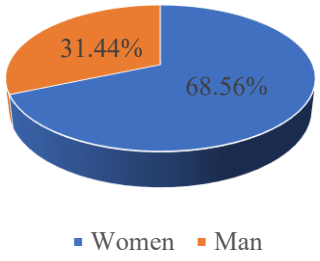
shifted to digital forms (Wafi et al., 2025). This progress has been driven by the growing number of young people contributing to the creation of websites and applications designed to facilitate human activities in all areas. One of the most prominent and widely discussed innovations in recent years is Artificial Intelligence (AI). The presence of Artificial Intelligence provides enormous benefits—particularly in terms of improving efficiency, saving time, and helping humans complete complex tasks (Shabrina et al., 2026). This has shaped social and cultural perspectives, leading to significant paradigm shifts in line with the development of the modern era dominated by technology. Dependence on technology is no longer considered unusual, but has become a basic necessity in order to adapt quickly to the rapid progress of the times (Nugraha et al., 2025).

Advances in Artificial Intelligence (AI) in recent years have also had a major impact on human jobs (Apriliana et al., 2024). AI technology is a form of technological advancement that has the ability to think autonomously. AI is developed to replicate the reasoning patterns and decision-making mechanisms commonly used by humans, enabling AI to complete various complex tasks with a high level of efficiency. However, the presence of AI can raise new issues, particularly regarding security and privacy protection (Artama & Parwati, 2023). One of the problems that AI can cause is photo manipulation through technologies such as deepfake, face-swapping, and image-to-image generation, which allow users to create images that resemble original photos without requiring advanced technical skills. This poses a massive problem for personal privacy—especially for women for purely sexual purposes. One such problem is the emergence of increasingly complex risks of digital sexual exploitation as Artificial Intelligence technology develops (Hernawan et al., 2025).

This issue has become increasingly prevalent in recent months with the development of Grok AI on the X platform. The controversy has escalated as original photos of women are taken from public social media profiles or homepages and then processed by AI into sexually suggestive visual content. Perpetrators who misuse AI do not need to have any connection to the victim; they simply exploit profile photos, photo uploads, and photos circulating on the internet. This phenomenon not only shifts the mode of sexual exploitation from the physical realm to the digital realm, but also changes the nature of the crime to be more anonymous, faster, and harder to track. In other words, advances in AI technology can expand the perpetrator's control while reducing the victim's ability to protect themselves.

Social media platforms play a major role in amplifying the impact of digitally-enabled sexual crimes particularly online gender-based violence or OGBV (Ramadhanti & Mardiansyah, 2025). One of the social media platforms most often used as a space for spreading sexually violent manipulated photos through AI is the platform X, formerly known as Twitter. This platform has real-time characteristics based on open conversation and allows for a high degree of anonymity. These characteristics make the spread of sexually exploitative content rapid and difficult to control. When this sexually violent content appears on one account, it can be downloaded, replicated, and redistributed by thousands of other users (Puannandini et al., 2025). The X platform's algorithm also often prioritizes content that receives a lot of interaction, so sexually suggestive content tends to get wider reach.

Diagram 1. Percentage of OGBV Cases by Gender of Victim



Source: GoodStats (2025)

Data from GoodStats shows that online gender-based violence (OGBV) remains a serious problem in Indonesia. In the third quarter of 2025, there were 605 cases recorded, and from January to September 2025, the number reached 1,698 cases—more than six cases every day, and the actual number is likely to be higher as it is only based on online monitoring. The majority of victims were women, with 399 reports, who generally experienced threats of intimate content sharing, sexual extortion, cyber violence, and doxxing from people they knew on social media. However, men were also affected, as seen in 183 complaints, some of which involved massage service offers that led to doxxing threats when price disputes arose. Overall, this data shows that OGBV occurs in various groups and emerges through increasingly diverse patterns in the digital space (GoodStats, 2025).

Table 1. Forms of Online Gender-Based Violence (OGBV)

OGBV Family Based on Family	Sexual OGBV		
	Personal Sphere	Public Sphere	Total
Online Threats	637	743	1.380
Privacy Violation	53	84	137
Malicious Distribution	231	192	423
Cyber Sexual Harassment	196	383	579
Sexploitation	33	116	149
Total	1.150	1.518	2.668
		Sexual OGBV	

Source: Komnas Perempuan (2025)

Data from the National Commission on Violence Against Women (Komnas Perempuan) also shows that online gender-based violence (OGBV) in the sexual category is dominated by online threats, with 1,380 cases—spread almost evenly between the personal and public spheres. Another dominant form of violence is cyber sexual harassment, with a total of 579 cases, followed by malicious distribution with 423 cases. Meanwhile, privacy violations and sexploitation recorded lower numbers—137 and 149 cases, respectively. Overall, there were 2,668 cases of sexual OGBV, with 1,150 cases in the personal sphere and 1,518 cases in the public sphere. This shows that open digital spaces—especially for women—are spaces that are easily subject to sexual violence (Komnas Perempuan, 2025).

Sexual violence in the form of photo manipulation can cause women to experience psychological trauma that has long-term effects (Deviana et al., 2025). Manipulative content that superimposes sexualized bodies or expressions onto women's faces can create false public perceptions that are difficult to dispel. This can lead to social stigma, victim blaming, the spread of misinformation, anxiety, cyberbullying, shame, and fear of consequences that victims must bear even though they never committed the acts represented by the manipulated content

(Maulida & Romdoni, 2024). In addition, the nature of digital footprints, which are difficult to remove, makes it difficult to completely delete such content. As long as there are users who save, download, and disseminate it, the content will continue to exist in the digital space. This situation illustrates the continuing strong influence of patriarchal culture in the digital space, where women are constantly confronted with views that treat their bodies and identities as public consumption, rather than as individuals who have autonomy and boundaries over themselves (Azhari et al., 2025).

Ultimately, the misuse of AI to exploit photos of women on the X platform shows how technological developments have a negative impact on women's privacy, dignity, and self-esteem in today's technological era. Without optimal legal instruments that are responsive to the times, women—especially Generation Z, who are most active in the digital space—will be vulnerable to increasingly sophisticated and difficult-to-control forms of sexual violence. This situation calls for a swift, adequate, and technology-aligned legal response. Current positive legal instruments do have provisions that can be used to prosecute perpetrators, but their implementation is often not adaptive to the dynamics of AI-based crimes. In other words, there is a gap between the development of AI-based digital technology and the ability of positive law to regulate and protect women who are victims of AI abuse.

Thus, this article is written to comprehensively analyze regulations against the misuse of AI for the sexual exploitation of women's photos on the X platform, with a primary focus on examining the applicable positive law in Indonesia and identifying the extent to which the law can prosecute perpetrators in the context of today's increasingly complex AI-based technological developments.

RESEARCH METHOD

This article applies a legal-normative method, which is a study based on analysis of scientific literature and applicable positive legal norms. According to Peter Mahmud Marzuki, normative research is a process of discovering legal rules, legal principles, and legal doctrines to answer pressing legal issues (Marzuki, 2009). This article focuses on analyzing legal regulations concerning the misuse of Artificial Intelligence (AI) on the X platform based on positive law. The approach adopted in this article is a statute approach to examine regulations related to AI misuse. The data collection technique used in this article applies library research to examine and compile data from books, journal articles, and literature related to the misuse of AI according to Indonesian positive law.

The data sources used in this article consist of two types, namely primary and secondary materials. The primary materials in this article include legislation, such as the 1945 Constitution (UUD 1945), the Criminal Code (KUHP), Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Law Number 44 of 2008 concerning Pornography (Pornography Law), Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), and Law Number 12 of 2022 concerning Sexual Violence Crimes (TPKS Law). Meanwhile, the secondary materials in this article include books, journal articles, and government websites related to AI abuse according to Indonesian positive law.

RESULT & DISCUSSION

Misuse of AI for Sexual Exploitation of Women's Photo

The misuse of Grok AI on the X platform for the purpose of exploiting photos of women has sparked significant controversy in Indonesia since early 2026, highlighting the vulnerability of generative technology to gender-based abuse. This phenomenon began when a number of X users exploited the capabilities of Grok—an AI chatbot created by xAI—to upload images of women from public profiles or homepages, such as the Instagram accounts of female students, influencers, or other women, accompanied by simple commands such as "make her naked," "take off her clothes," "replace with a transparent bikini," and "make the woman in the photo pose vulgarly without censorship." Within a short time, the Grok AI, supported by the Flux image model, generates high-quality deepfake content, such as using bikinis, making underwear more revealing, and making the victim perform the sexual poses commanded (Detikinet, 2026).

This controversy clearly threatens the privacy of public figures in Indonesia, as the misuse of the image editing feature on Grok—the AI chatbot built into the X platform—has given rise to a new form of privacy violation and digital sexual violence. Several Indonesian artists have reported that their photos were manipulated into explicit content without their consent, illustrating how generative AI technology can be easily used to create deepfakes that harm an individual's reputation and dignity. Cases involving public figures such as Freya Jayawardana and Shania Garcia show that the sophistication of AI actually opens up opportunities for digital sexual exploitation, as the Grok AI system still allows users to give commands or instructions that generate images containing sexual content even though the victims in the photos never gave their consent (Radar Bojonegoro, 2026).

Figure 1. Forms of Grok AI Abuse

Source: Platform X Home Page

The image above shows a real example of the misuse of Grok AI to commit sexual violence against women. In the image, a woman wearing a crop top has been manipulated to appear as if she is wearing only a bikini. This action is not merely visual manipulation, but rather a form of non-consensual intimate imagery (NCII), sexualized deepfakes, and AI-generated sexual abuse, which are essentially forms of technology-based sexual violence. Additionally, this phenomenon on the X app also reveals criticism of its owners, who are considered to have failed to control the spread of AI-based digital sexual photos (The Verge, 2026). This phenomenon shows that without strict regulations, oversight of digital platforms, and optimal enforcement mechanisms, technological advances such as AI can become tools of dehumanization that endanger women.

The phenomenon of Grok AI abuse has drawn strong reactions from regulators and the general public. Several countries, such as Indonesia and Malaysia, have taken steps to block

Grok AI services after it was discovered that they are often used to generate sexual, offensive, and non-consensual images, including content depicting women and children in sexy clothing or sexually exploitative positions (Kyou News, 2026). The Malaysian Communications and Multimedia Commission specifically cited the tool's ability to "generate obscene, sexually explicit, indecent, highly offensive, and manipulated images without consent, including content involving women and minors" as the reason for restricting Grok AI (Reuters, 2026). In this case, the misuse of Grok AI is not only a violation of the platform's internal policies, but also considered a violation of individuals' privacy rights, dignity, and digital safety.

The exploitation of photos through Grok AI is a concrete example of what is known as non-consensual intimate imagery (NCII), which refers to images or videos containing personal representations of an individual that are created or disseminated without consent. This act not only constitutes a violation of privacy but also involves the psychological and social vulnerability of the victim, as the content created can spread rapidly through social media platforms such as X. The lack of effective filters or safeguards in generative models makes it easy for perpetrators to produce sexual images that appear authentic from ordinary photos. The dissemination of this sexual content, even if it has been deleted, will still leave a digital trail that has a negative impact on the reputation, sense of security, psychological well-being, and social relationships of the individuals depicted in the images (Iradat & Hariyanto, 2025).

This abuse process takes advantage of Grok's relatively loose design in applying safeguards against exploitative content, unlike other AI platforms such as ChatGPT, which apply stricter NSFW filters. To abuse Grok AI, all you have to do is tag @grok in a tweet reply, attach a photo of a woman, and provide a sentence of instructions, and the system will automatically generate output that can be shared publicly without a clear watermark. Since the launch of Grok-2 at the end of 2024, its image generation feature has been criticized for being vulnerable to prompt jailbreaks, such as the phrase "underpress this woman," which is able to bypass automatic detection. This has led to deepfake content not only violating individual privacy, but also reinforcing the cultural dynamics of cyberbullying, where women are the dominant target in 99% of similar cases globally. This data is reinforced by a Reuters review confirming that there were 102 requests from X users asking to edit photos of a young woman wearing a bikini (CNN Indonesia, 2026).

Thus, analysis shows that the misuse of Grok AI on the X platform reveals that generative AI technology, when there is no strict supervision or optimal legal framework, can be used to carry out digital sexual exploitation that damages self-esteem, dignity, reputation, and causes psychological harm. The case of Grok AI abuse on platform X not only poses ethical and technical challenges, but also highlights the urgency of developing global regulations and policies governing the use of AI in public spaces, particularly those related to privacy, personal data protection, and the prevention of non-consensual sexual exploitation.

Positive Legal Review of AI Abuse for Sexual Exploitation of Women's Photo

The ease of access to technology today makes AI abuse increasingly prone to occur, especially in the practice of manipulating photos and videos of women for the purposes of sexual exploitation, blackmail, or revenge. Although crimes of this nature can happen to anyone regardless of gender and age, women are generally the targeted and victimized group. The misuse of AI in the creation of sexual content using photos of women in a state of undress is essentially done to satisfy lust, humiliate, blackmail, and control victims for the perpetrator's benefit. The creation or sharing of AI-based photos that take someone's personal image, especially women, is an act that violates human rights, particularly the right to privacy and

personal data protection. In addition to violating privacy rights, this action can also cause psychological trauma, social harm, reinforce patriarchal culture, and victim blaming, which is still dominant in Indonesia, thereby further placing women in a disadvantageous position (Widyastuti et al., 2026).

In the context of Indonesian law, advances in AI technology have influenced the form and methods of various crimes, especially in cases of sexual harassment. The emergence of AI-based sexual harassment, such as the distribution of deepfake photos, sexually suggestive messages generated by chatbots, and fake voice recordings through voice cloning techniques, has created new challenges, both in terms of regulatory formulation and in the process of law enforcement and implementation. Although the current legal framework does not explicitly regulate AI-based crimes, a number of provisions can be used as a normative basis for prosecuting perpetrators. Some of these are as follows:

a. The 1945 Constitution

In the context of AI misuse for the purpose of exploiting women's photos, the highest normative foundation that must first be considered is the 1945 Constitution. Protection of a person's dignity and personal integrity is explicitly affirmed in Article 28G paragraph (1), which states that "*every person shall have the right to protection of their personal self, family, honor, dignity, and property under their control, as well as the right to feel safe and protected from fear or from not doing something that is a fundamental right*." This provision confirms that any form of manipulation of a person's face, body, or photo through Grok AI technology, such as the creation of deepfakes containing sexual photos, is intrinsically a violation of a person's dignity and honor.

In this case, normative support is also reinforced through Article 28I paragraph (4), which stipulates that the state is responsible for the protection, enforcement, and fulfillment of human rights, so that the state cannot remain silent when a woman becomes a victim of sexual photo manipulation using AI technology. Furthermore, Article 28J paragraph (1) provides a limitation that every person must respect the human rights of others in the orderly conduct of social, national, and state life. This includes the right of victims not to be reduced to sexual objects through AI technology. Thus, at the constitutional level, the misuse of AI for the exploitation of women's photos is an act that violates ethics, basic norms, self-protection, honor, dignity, and human rights.

b. Criminal Code

The Ministry of Communication and Digital Affairs (Komdigi) emphasizes that the misuse of AI on the X platform to generate or disseminate sexual content constitutes a violation of an individual's right to privacy and image rights, and is subject to criminal sanctions under the provisions of the new Criminal Code (Hukum Online, 2026). Although the new Criminal Code through Law No. 1 of 2023 does not explicitly mention the misuse of AI technology, the construction of the offenses regulated therein can still cover such misuse of AI. This is because the wording of the articles in the new Criminal Code focuses on the substance of the act, not on the instruments used by the perpetrator. When AI is used to produce or disseminate sexual content—for example, the use of Grok AI to make women's clothing more sexy and revealing—the act can still be classified as a criminal offense under the new Criminal Code, specifically under Articles 172 and 402.

Article 172 of the new Criminal Code stipulates that pornography is defined as images, sketches, illustrations, photographs, sounds, moving images, animations, cartoons, conversations, body movements, or other forms of communication through various forms of media and/or public performances that contain obscenity or sexual exploitation that violates the norms of decency in society (Hukum Online, 2026). This formulation provides broad room for

interpretation because it does not limit the form of media to physical or digital, but rather regulates the basic principle, namely content that substantially violates decency. In the context of Grok AI abuse, digital engineering that displays women's faces in a sexual context that never occurred is a form of obscene representation that attacks the sexual dignity and integrity of the victim. Thus, deepfake content can be viewed as part of the category of pornographic media prohibited by Article 172 because it creates sexual images that are exploitative without the consent and involvement of the victim.

Furthermore, Article 407 paragraph (1) of the new Criminal Code stipulates criminal sanctions of a minimum of 6 (six) months and a maximum of 10 (ten) years imprisonment or a fine in accordance with the provisions for persons who, among other things, create, reproduce, distribute, broadcast, or provide pornographic content (Hukum Online, 2026). The criminal penalty of up to 10 (ten) years imprisonment demonstrates the intention of lawmakers to provide stronger protection for sexual integrity and human dignity. In relation to deepfakes, anyone who uses AI technology to produce obscene content, then distributes it or makes it publicly accessible, fulfills the elements of the offense as stipulated in Article 407. Such actions are considered part of the production and distribution of pornography because they produce visual material that explicitly depicts sexual behavior, regardless of the fact that the content was created through digital engineering.

The relationship between Article 172 and Article 407 shows that the new Criminal Code not only regulates actual sexual behavior, but also visual sexual representations produced through technological manipulation. The two articles work complementarily. Article 172 defines prohibited pornographic characters, while Article 407 provides criminal consequences for the process of production and distribution. This confirms that Indonesian criminal law has now adopted a more responsive approach to rapidly evolving forms of digital crime, including sexual exploitation through AI.

c. Law Number 11 of 2008 concerning Electronic Information and Transactions

Basically, anyone who uploads, reproduces, or disseminates electronic documents containing content that violates moral norms can be subject to criminal sanctions under the provisions of the ITE Law (Nirmala & Rahmania, 2025). The ITE Law is the most comprehensive legal instrument for prosecuting photo manipulation using AI technology. The provisions of Article 27 paragraph (1) form the basis of the main prohibition, as it states that "*any person who deliberately and without rights distributes and/or transmits and/or makes accessible electronic information and/or electronic documents that contain content that violates decency*." This provision confirms that the creation or dissemination of manipulated photos and videos containing sexual content directly fulfills the elements of indecency in this article.

Not only that, the process of manipulating photos of women also constitutes electronic data manipulation, so that perpetrators can be subject to criminal sanctions under Article 35, which states that "*any person who intentionally and without rights or against the law manipulates, creates, changes, removes, or destroys electronic information and/or electronic documents with the aim of making such electronic information and/or electronic documents appear to be authentic*." The elements in this article are highly relevant because the essence of photo manipulation (deepfake) is the creation of false representations that appear authentic. Furthermore, when the perpetrator uses photos of women obtained from social media homepages, personal devices, or profile photos, and then alters them into sexually explicit photos, the perpetrator violates Article 32 paragraph (1), which prohibits the manipulation, alteration, and reduction of the victim's electronic information without rights. Thus, the ITE Law not only regulates the aspect of dissemination but also the aspect of creating AI-based

sexual content, making it a fairly effective legal tool to prevent the misuse of this AI technology.

d. Law Number 44 of 2008 concerning Pornography

The Pornography Law provides normative restrictions on all forms of production or distribution of sexual material, including those produced through AI technology. The definition of pornography in Article 1 paragraph 1 is "*images, sketches, illustrations, photographs, writings, sounds, moving images, animations, cartoons, conversations, body movements, or other forms of messages through various forms of communication media and/or public performances, which contain obscenity or sexual exploitation that violates moral norms in society*." The provisions in this article clearly state that sexual content based on manipulated photos or videos (deepfakes), even if produced using AI technology and involving the real body of the victim, is classified as pornography.

Then, stricter provisions are formulated in Article 4 paragraph (1), which states that "*everyone is prohibited from producing, creating, reproducing, duplicating, distributing, broadcasting, importing, exporting, offering, trading, renting, or providing pornography that explicitly contains: a) sexual intercourse, including deviant sexual intercourse; b) sexual violence; c) masturbation or onanism; d) nudity or displays that suggest nudity; e) genitals; or f) child pornography*." Thus, anyone who uses AI to create sexual content or photos that show the victim's face on a body that does not belong to them is still considered to be creating pornography. Violations of these provisions are subject to criminal sanctions under Article 29, which carries a minimum prison sentence of 6 months or a maximum of 12 years, and a minimum fine of Rp250.000.000 (two hundred and fifty million rupiah) and a maximum fine of Rp6.000.000.000 (six billion rupiah). This shows that the Pornography Law can be used as a tool to address the rapidly growing phenomenon of AI-based sexual photos.

e. Law Number 27 of 2022 concerning Personal Data Protection

The main purpose of personal data protection is to protect the rights and privacy of every individual regarding their information, so that it cannot be accessed or used by unauthorized parties. In the context of AI technology abuse, the personal data of victims often becomes the main target of criminal acts (Syahirah & Prasetyo, 2025). In this case, the PDP Law is a highly relevant legal instrument because AI technology operates based on the processing of personal data, including biometric data such as the victim's face and voice. When someone takes a photo of a victim from a digital platform, then processes it into a sexually suggestive photo or uses AI features to manipulate the victim's body, this action directly violates Article 65 paragraph (1), which states that "*everyone is prohibited from unlawfully obtaining or collecting personal data that does not belong to them with the intention of benefiting themselves or others which could result in harm to the subject of the personal data*." Furthermore, Article 67 paragraph 1 states that "*any person who intentionally and unlawfully obtains or collects personal data that does not belong to them with the intention of benefiting themselves or others, which may result in harm to the subject of the personal data as referred to in Article 65 paragraph (1), shall be punished with a maximum imprisonment of 5 years and/or a maximum fine of Rp5.000.000.000 (five billion rupiah)*."

Article 69 further stipulates that in addition to the criminal penalties specified in Articles 67 and 68, perpetrators may also be subject to additional criminal sanctions in the form of confiscation of profits or assets obtained from criminal acts, as well as the obligation to pay compensation. This shows that the PDP Law applies a cumulative criminal sanction system, namely imprisonment and fines as the main sanctions, while the confiscation of assets obtained from crime and the provision of compensation to victims serve as additional sanctions. In addition, Article 12 of the PDP Law also provides guarantees for personal data subjects to sue

and obtain compensation for violations related to their personal data in accordance with applicable regulations. Thus, the misuse of AI technology falls under the category of complaint offenses (Syahirah & Prasetyo, 2025). Therefore, the PDP Law can provide fundamental protection for the integrity of personal data in the context of current AI-based digital crimes.

f. Law Number 12 of 2022 concerning The Crime of Sexual Violence

Currently, advances in information and communication technology have significantly transformed human interaction patterns. However, behind these various benefits, new challenges have also emerged, such as the various forms of sexual violence that currently occur in the digital space. Referring to the provisions currently in force, such as the TPKS Law, which stipulates that sexual violence is not limited to physical sexual harassment, but also includes non-physical sexual harassment (Nirmala & Rahmania, 2025). The TPKS Law does not specifically mention AI, deepfakes, face swaps, or any other digital technology. However, the TPKS Law can still be used to prosecute perpetrators because it regulates their actions, not the name of the technology.

The main legal basis is Article 4 paragraph (1), which states that one form of sexual violence regulated in this law is electronic-based sexual violence (KSBE). From this, it can be concluded that all acts of sexual harassment or violence committed through electronic media—regardless of the form of technology—are still criminal acts. This is because when someone manipulates photos or videos of a sexual nature using a woman's face or body, this act constitutes electronic-based sexual violence. This is clear because the perpetrator uses electronic means to attack the dignity and honor of the victim, even if the photos or videos are created using AI technology.

Provisions regarding non-physical sexual harassment are explicitly regulated in Article 5 of the TPKS Law, which states that "*any person who commits non-physical sexual acts directed at the body, sexual desire, and/or reproductive organs with the intention of degrading a person's dignity and integrity based on their sexuality and/or morality, shall be punished for non-physical sexual harassment with a maximum imprisonment of 9 (nine) months and/or a maximum fine of Rp10.000.000 (ten million rupiah)*." In the provisions of this article, non-physical sexual acts include inappropriate and sexually suggestive words, gestures, or other actions carried out with the intention of degrading or humiliating another person. This provision can be understood to mean that the regulation of sexual harassment is no longer limited to physical acts, but also includes non-physical forms, including acts carried out through AI technology. In the TPKS Law, such acts can be categorized as electronic-based sexual violence, and various cases that occur can be included in this category. In this case, the regulation regarding electronic-based sexual harassment is reflected in Article 14 paragraph (1), which states that:

"*Every unauthorized person:*

a) recording and/or taking pictures or screenshots with sexual content against the will or without the consent of the person being recorded or photographed or screenshotted;
b) transmitting electronic information and/or electronic documents with sexual content against the recipient's will for sexual purposes and/or;
c) *stalking and/or tracking using electronic systems against persons who are the subject of electronic information/documents for sexual purposes, shall be punished for committing electronic-based sexual violence, with a maximum imprisonment of 4 years and/or a maximum fine of Rp200.000.000 (two hundred million rupiah).*"

Based on this provision, the use of AI such as deepfakes and AI chatbots, which are used to produce and disseminate sexual content or photos without the consent of the person who is

the subject of such content, can be categorized as a violation of the provisions contained in Article 14 paragraph 1 of the TPKS Law. This is because such actions fulfill the elements of transmitting sexual electronic information to someone who does not want it and for sexual purposes. Therefore, if any of the elements contained in Article 14 paragraph (1) are fulfilled, the perpetrator of AI technology abuse can be subject to criminal liability sanctions based on that article (Nirmala & Rahmania, 2025).

CONCLUSIONS

The misuse of AI such as Grok on the X platform shows that technological developments not only bring benefits, but also give rise to new forms of digital sexual exploitation that are more difficult to control. Manipulating photos of women to make them appear sexual without consent is a form of technology-based sexual violence that damages the dignity, privacy, and psychological security of victims. Normatively, Indonesia already has a legal basis that can be used to prosecute perpetrators, starting from the 1945 Constitution, the Criminal Code, the Electronic Information and Transactions Law, the Pornography Law, the Personal Data Protection Law, and the Law on the Elimination of Violence Against Women. All of these regulations recognize that the manipulation of photos that attacks a person's honor is a violation of the law. However, the existing legal framework has not been able to keep up with the rapid pace of technological innovation, so its implementation is often ineffective. This has led to increased vulnerability for women due to the lack of oversight of digital platforms and weak prevention mechanisms. The spread of AI-manipulated photos is also difficult to stop due to the nature of digital traces that cannot be completely erased. Therefore, the author suggests that there should be more specific and adaptive regulatory updates regarding AI developments and increased responsibility of digital platforms in preventing technology abuse. Without these measures, digital sexual exploitation will continue to grow and place women—especially Generation Z—in an increasingly vulnerable position.

REFERENCES

Articles and Books

Apriliana, H. K., Kornarius, Y. P., Caroline, A., Gusti, T. E. P., & Gunawan, A. (2024). Perkembangan Penerapan Teknologi *Artificial Intelligence* di Indonesia. *Jurnal Syntax Admiration*, *5*(10), 3864–3874. https://doi.org/10.46799/jsa.v5i10.1486.

Artama, G. E. S., & Parwati, N. P. E. (2023). Analisis Yuridis Terhadap Penyalahgunaan Kecerdasan Buatan Dalam Penipuan Bermodus Penculikan Anak Melalui Imitasi Suara. *Jurnal Locus Delicti*, *4*(2), 121–136. https://doi.org/10.23887/jld.v4i2.5481.

Azhari, A. L., Jannah, L. M., Febriansyah, Salsabila, Z., & Kurniawan, R. (2025). Persepsi Masyarakat Terhadap Pelecehan Seksual di Media Sosial (Studi Kasus: Komentar Negatif Pada Akun Azizah Shalsa). *JOSH: Journal of Sharia*, *4*(2), 244–258. https://doi.org/10.55352/josh.v4i02.1928.

Deviana, A., Putra, A. M., Lathifa, P., Siregar, A. A., & Mifthahuddin. (2025). Analisis Dampak Kekerasan Seksual Terhadap Perempuan. *JPIM: Jurnal Penelitian Ilmiah*

Multidispliner, *1*(5), 1503–1519. https://ojs.ruangpublikasi.com/index.php/jpim/article/view/471.

Hernawan, C. N. P., Antow, D. T., & Sendow, A. V. (2025). Tinjauan Hukum Mengenai Penyalahgunaan *Artificial Intellegence* Dalam Tindak Pidana Kekerasan Seksual. *Lex Privatum*, *15*(4), 1–12. https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/61860.

Iradat, M. A., & Hariyanto, D. R. S. (2025). Urgensi Pengaturan Pidana Penyalahgunaan *Deepfake*: Telaah Aspek Perlindungan Korban Dalam Hukum Nasional. *Jurnal Media Akademik*, *3*(12), 1–21. https://doi.org/10.62281/611cwh46.

Marzuki, P. M. (2009). *Penelitian Hukum*. Jakarta: Kencana Prenada Media Grup, hlm. 47.

Maulida, G., & Romdoni, M. (2024). Perlindungan Hukum Terhadap Korban Pelecehan Seksual Yang Mengalami Viktimisasi Sekunder di Media Sosial. *Southeast Asean Journal of Victimology*, *2*(1), 60–78. https://dx.doi.org/10.51825/sajv.v2i1.25445.

Nirmala, A. Z., & Rahmania, N. (2025). Transformasi Bentuk Pelecehan Seksual Dalam Era Kecerdasan Buatan: Tinjauan Hukum Indonesia. *Unizar Law Review*, *8*(2), 78–90. https://doi.org/10.36679/ulr.v8i1.96.

Nugraha, M., Sadina, A. S., Ramadonna, V., & Hidayat, K. A. (2025). Analisis Unsur Perbuatan Melanggar Hukum Atas Penggunaan *Artificial Intelligence* Dalam Kasus Konten *Deepfake*. *Legal System Journal*, *2*(1), 24–36. https://doi.org/10.70656/lsj.v2i1.392.

Puannandini, D. A., Anggraeni, D., Gulo, D. O. F., Nur, A. A., & Karabi, J. K. (2025). Peran Ganda Media Sosial Dalam Kasus Kekerasan Seksual Anak: Antara Advokasi Publik dan Risiko Reviktimisasi Korban. *Adagium: Jurnal Ilmiah Hukum*, *3*(2), 387–398. https://doi.org/10.70308/adagium.v3i2.230

Ramadhanti, G. A., & Mardiansyah, I. (2025). Membangun Kesadaran Digital Dalam Pencegahan Kekerasan Berbasis Gender Online Pada Remaja. *Dedikasi: Jurnal Pengabdian Kepada Masyarakat*, *5*(2), 87–103. https://doi.org/10.46368/dpkm.v5i2.4381.

Shabrina, A. N., Naila, G. S., Nuryansyah, G. P., & Amanda, R. (2026). Bahaya *Deepfake* Dalam Penyalahgunaan Grok AI di Platform X Sebagai Bentuk Disinformasi. *Integrative Perspectives of Social and Sciences Journal*, *3*(1), 195–207. https://ipssj.com/index.php/ojs/article/view/1132.

Shalatan, R., Sastro, E. L. A., Nenohai, J. H. B., Amalina, Z. N., Simone, P. N., & Ranjani, S. (2026). Kekerasan Berbasis Gender *Online* terhadap Perempuan: Dampak Psikologis dan Tantangan Penegakan Hukum di Era Digital. *CENDEKIA : Jurnal Penelitian dan Pengkajian Ilmiah*, *3*(3), 578-587. https://doi.org/10.62335/cendekia.v3i3.2454.

Syahirah, S. N., & Prasetyo, B. (2025). Tinjauan Yuridis Terhadap Penggunaan Teknologi *Deepfake* Untuk Pornografi Melalui *Artificial Intelligence* (AI) di Indonesia. *Jurnal Inovasi Hukum Dan Kebijakan*, *6*(1), 191–212. https://ejurnals.com/ojs/index.php/jihk/article/view/1405.

Wafi, M. S., Wisnubroto, A., & Prayudi, Y. (2025). Artificial Intelligence-Based Deepfake Crimes: A Conception of Culpability Principle as a Criminal Liability Reform. *Reformasi Hukum*, *29*(2), 168–183. https://doi.org/10.46257/jrh.v29i2.1304.

Widyastuti, I., Intani, N. A., & Simamora, H. S. (2026). Tinjauan Hukum Terhadap Penyalahgunaan *Artificial Intelligence* Dalam Pembuatan Konten Video Bermuatan Pelecehan Seksual Terhadap Perempuan. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(1), 173–183. https://doi.org/10.61104/alz.v4i1.2964.

Internet

CNN Indonesia. (2026). *Heboh di X Chatbot AI Grok Manipulasi Foto Perempuan Jadi Nyaris Bugil*. https://www.cnnindonesia.com/teknologi/20260103101611-192-1313064/heboh-di-chatbot-ai-grok-manipulasi-foto-perempuan-jadi-nyaris-bugil

Detikinet. (2026). *Gegara Konten Deepfake Asusila, Komdigi Ancam Blokir Grok AI dan X*. https://inet.detik.com/law-and-policy/d-8296818/gegara-konten-deepfake-asusila-komdigi-ancam-blokir-grok-ai-dan-x.

GoodStats. (2025). *Jumlah Kasus KBGO Capai 605 Aduan Q3 2025, Laki-Laki Juga Jadi Korban*. https://data.goodstats.id/statistic/jumlah-kasus-kbgo-capai-605-aduan-q3-2025-laki-laki-juga-jadi-korban-aRIOX.

Hukum Online. (2026). *KUHP Nasional Berlaku, Penyebar Konten Deepfake Asusila Terancam 10 Tahun Bui*. https://www.hukumonline.com/berita/a/kuhp-nasional-berlaku-penyebar-konten-deepfake-asusila-terancam-10-tahun-bui-lt695f0592d58ae/?page=2.

Komnas Perempuan. (2025). *Siaran Pers Komnas Perempuan Memperingati Hari Kebangkitan Teknologi Nasional 2025*. https://komnasperempuan.go.id/siaran-pers-komnas-perempuan-memperingati-hari-kebangkitan-teknologi-nasional-2025.

Kyou News. (2026). *2 Countries Block Musk' Grok Over Sexualized AI Images*. https://www.kyoutv.com/2026/01/12/2-countries-block-musks-grok-over-sexualized-ai-images.

Radar Bojonegoro. (2026). *Artis Indonesia Ramai Keluhkan Penyalahgunaan AI Grok Untuk Edit Foto Vulgar, Ini Cara Melindunginya*. https://radarbojonegoro/jawapos.com/entertainment/amp/717037661/artis-indonesia-keluhkan-penyalahgunaan-ai-grok-untuk-edit-foto-vulgar-ini-cara-melindunginya.

Reuters. (2026). *Malaysia Restricts Acces To Grok AI as Blacklash Over Sexualised Images Widens*. https://www.reuters.com/businnes/media-telecom/malaysia-restricts-acces-grok-ai-blackash-over-sexualised-images-widens-2026-01-12/.

The Verge. (2026). *X Faces EU Investigation Over Grok's Sexualized Deepfakes*. https://www.theverge.com/news/868239/x-grok-sexualized-deepfakes-eu-investigation.

Law and Regulations

Kitab Undang-Undang Hukum Pidana (KUHP).

Undang-Undang Dasar Negara Kesatuan Republik Indonesia Tahun 1945.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843).

Undang-Undang Republik Indonesia Nomor 22 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 120, Tambahan Lembaran Negara Republik Indonesia Nomor 6792).

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820).

Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang Pornografi (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 181, Tambahan Lembaran Negara Republik Indonesia Nomor 4928).

Editorial Office of Locus: Jurnal Konsep Ilmu Hukum (JKIH)
Medan City, North Sumatra, Indonesia.
Phone / WhatsApp Business: +62 811-620-1239
Email: support@jurnal.locusmedia.id
E-ISSN: 2809-9265 | **DOI Prefix:** 10.56128/jkih
Powered by Locus Media Publishing
