

CHAPTER I

INTRODUCTION

A. Background

In today's digital age, society is witnessing the emergence of technologies that are revolutionary but also bring new challenges in understanding and addressing the adverse impacts that the use of these technologies can have.¹ Technology and the internet provide humans with the opportunity to create more advanced, intelligent, and cost-effective mechanisms. One example is the creation of artificial intelligence. Artificial intelligence is one example of current technological developments. Artificial intelligence (AI) is formed from two words: “artificial,” which means not real, and “intelligence,” which means smart.²

Artificial intelligence was created with the aim of helping humans to make their work easier. Artificial intelligence was initially only capable of processing simple commands, but now it can understand more complex commands such as understanding human language, recognizing human faces, driving vehicles, and even faking human voices and faces. In response to this, companies have emerged that create programs that use artificial intelligence as their main interest.³

¹ L. Huang and J. Ren, “The Negative Impact of Emerging Technology: A Literature Review,” in Proceedings of the International Conference on E-Business and E-Government (ICEE 2010), 2010, 2576–2579, <https://doi.org/10.1109/ICEE.2010.651>

² Jufri and Putra, “Aspek Hukum Internasional dalam Pemanfaatan Deepfake Technology terhadap Perlindungan Data Pribadi,” *Uti Possidetis: Journal of International Law*, 36.

³ Luh Putu Ary Sri Tjahyanti, Putu Satya Saputra, and Made Santo Gitakarma, “Peran Artificial Intelligence (AI) untuk Mendukung Pembelajaran di Masa Pandemi Covid-19,” *KOMTEKS* 1, no. 1 (2022): 16.

The phenomenon of "deepfakes", which includes advanced digital manipulation using artificial intelligence, has affected the way people interact with information, media, and each other online.⁴ On the one hand, technology provides convenience and positive benefits. However, on the other hand, this progress also brings challenges such as over-dependence, misuse, the spread of false information, and privacy issues that can have negative effects on society itself.⁵

Artificial Intelligence (AI) is a technology that can be used by humans as a tool to support activities carried out by humans themselves. Functionally, Artificial Intelligence has more or less the same function as a robot, however, Artificial Intelligence comes in a different appearance in the form of a computer system displayed in visual form. It can be said that Artificial Intelligence is the brain of a robot.⁶ Artificial Intelligence (AI) can perform various abilities such as understanding the commands given by humans. Indonesia is showing rapid progress in the development of Artificial Intelligence (AI). According to liputan6.com, Indonesia is one of the countries that has contributed significantly to the use of Artificial Intelligence (AI), as evidenced by the fact that Artificial Intelligence has been utilized by 22.1 percent of workers in various sectors in Indonesia.⁷

⁴ Karnouskos, S. "Artificial Intelligence in Digital Media: The Era of Deepfakes." *IEEE Transactions on Technology and Society* 1, no. 3 (July 2020): 138–147. <https://doi.org/10.1109/TTS.2020.3001312>

⁵ Hapsari, Rian Dwi, and Kuncoro Galih Pambayun. "Ancaman Cybercrime Indonesia: Sebuah Tinjauan Pustaka Sistematis." *Jurnal Konstituen* 5, no. 1 (2023): 3–4.

⁶ Pratikno, A. S. "Implementasi Artificial Intelligence dalam Memetakan Karakteristik, Kompetensi, dan Perkembangan Psikologi Siswa Sekolah Dasar Melalui Platform Offline Conference." In *Proceeding KMP Education Research Conference Keluarga Mahasiswa Pascasarjana (KMP)*, 18–27. September 2017.

⁷ G. D. Prasasti, "Wamenkominfo: 22,1 Persen Pekerja di Indonesia Sudah Mulai Menggunakan AI," *Liputan6*, June 8, 2024,

Deepfake is a human image engineering technology or synthetic technique based on Artificial Intelligence (AI).⁸ Marissa Koopman (et.al) explains deepfake as follows:⁹ “*the deepfake algorithm allows users to replace the face of one actor in a video with the face of a different actor in a photorealistic manner*”. In other words, deepfake is a term given to an algorithm, which allows users to change the face of one actor into the face of another actor in a video that is photorealistic¹⁰ to be specific, imitating a real visual object.¹¹

The manipulation of images in this matter will certainly harm the source subject whose identity has been faked. Moreover, the majority of cases of personal data manipulation involving photographs by other individuals are carried out without the consent of the source subject. This element of without rights is a crucial factor in identifying whether such actions constitute a criminal offense or not.¹² In addition, the source subject's position as the data owner becomes at risk because they must bear the consequences and damages caused by the content.¹³

Another issue that is just as significant as how deepfake pornographic image manipulation content is created is how quickly such content spreads,

<https://www.liputan6.com/tekno/read/5467690/wamenkominfo-221-persen-pekerja-di-indonesia-sudah-mulai-pakai-ai?page=2>

⁸ Khusna, I. H., & Pangestuti, S. (2019). *Deepfake, Tantangan Baru Untuk Netizen*. *Jurnal Promedia*, Vol. 5, No. 2, 2019: 2.

⁹ M. Koopman et al., “Detection of Deepfake Video Manipulation,” in *Proceedings of the 20th Irish Machine Vision and Image Processing Conference* (2018), 133.

¹⁰ I. D. Kasita, “Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) di Era Pandemi Covid-19,” *Jurnal Wanita dan Keluarga* 3, no. 1 (2022): 18.

¹¹ Lysy C. Moleong (et.al). “Implementasi Cluster Computing Untuk Render Animasi,” *E-Jurnal Teknik Elektro dan Komputer*, Vol. 2, No. 3 (2013): 4.

¹² Jufri and Putra, “Aspek Hukum Internasional dalam Pemanfaatan Deepfake Technology terhadap Perlindungan Data Pribadi,” *Uti Possiditis: Journal of International Law*, 36.

¹³ Van Apeldorn, *Pengantar Ilmu Hukum*, 17th ed. (Jakarta: PT Grafitas, 1981), 102.

especially if it looks authentic and credible. The public is not yet fully aware of the need to verify information found on the internet, which means that false content or hoaxes can spread quickly.¹⁴

The rise of deepfakes has brought about a new set of regulatory challenges and considerations. Regulators must meet the moment to provide guardrails for the use of technology as it scales while negotiating the interests of tech companies, arts companies, healthcare, consumers, and other stakeholders. One of the biggest challenges in enforcement is catching the most malicious users, who often operate anonymously, adapt quickly, and share their synthetic creations through borderless online platforms.¹⁵ Other than the video version, deepfake technology can also be used to manipulate an image.¹⁶

Then, deepfake technology is often used to abuse, which can lead to crimes such as the use of deepfake technology in spreading pornographic content. This is known as deepfake-based pornography.¹⁷ Furthermore, deepfake-based pornography perpetrators will steal the victim's bodily authority by making the victim do something that the perpetrator wants without the victim's permission and even knowledge. This is considered a criminal act, where the perpetrator commits several crimes at once when making deepfake-based pornography.¹⁸

¹⁴ Albert Lodewyk Sentosa Siahaan, "Urgensi Perlindungan Data Pribadi di Platform Marketplace terhadap Kemajuan Teknologi," *Majalah Hukum Nasional* 52, no. 2 (2022): 72.

¹⁵ A. Lawson, "A Look at Global Deepfake Regulation Approaches," *Responsible AI*, April 25, 2024, <https://www.responsible.ai/a-look-at-global-deepfake-regulation-approaches/>

¹⁶ E. I. Utawi and N. Ruhaeni, "Penegakan Hukum terhadap Tindak Pidana Pornografi menurut Peraturan Perundang-undangan tentang Pornografi melalui Media Sosial," *Bandung Conference Studies: Law Studies* 3, no. 1 (2023): 368.

¹⁷ I. D. Kasita, "Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) di Era Pandemi Covid-19," *Jurnal Wanita dan Keluarga* 3, no. 1 (2022): 17

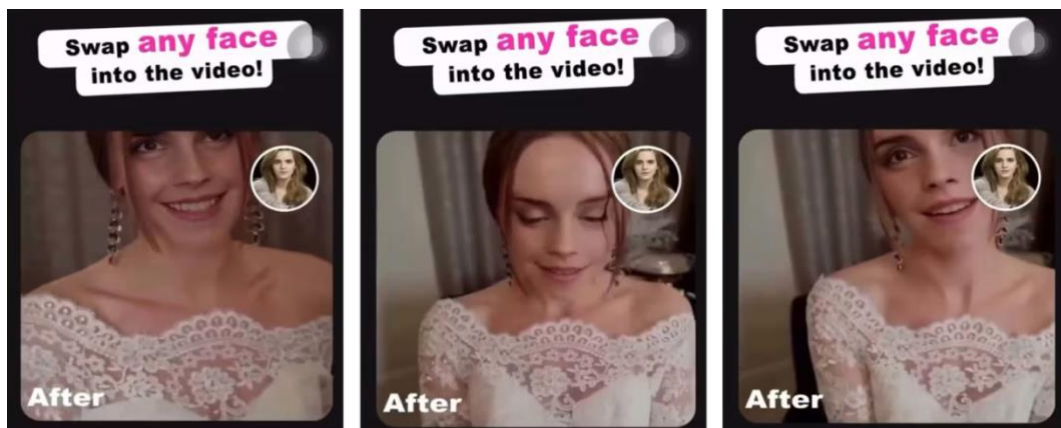
¹⁸ I. D. Kasita, "Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) di Era Pandemi Covid-19," *Jurnal Wanita dan Keluarga* 3, no. 1 (2022): 22



In Indonesia, one of the phenomena that became the starting point for the recognition of deepfake-based pornography among the public was the case that happened to a student of the Faculty of Economics and Business, Udayana University (FEB Unud) with the initials SLKDP was published in the media. The perpetrator allegedly committed sexual harassment by creating “deepfake” pornographic content. The perpetrator's modus operandi involved stealing photos of women from their Instagram accounts. These photos were then edited to appear nude using an artificial intelligence (AI)-based bot on Telegram. The perpetrator's former legal counsel, Bayu Wicaksono, stated that the case was uncovered after the perpetrator's girlfriend (who exposed the incident) sent one of the edited images to the victim. The victims' parents subsequently contacted the perpetrator's parents to discuss the matter. Both parties met on March 18, 2025. “At the meeting, several parents of the victims who were present

requested the creation of an apology video, a public apology through media advertisements, and a formal statement signed before a notary,” said Bayu when contacted. In this case, at least 35 female students from Udayana University (Unud) have reported to the university administration that they were victims of the perpetrator’s deepfake pornographic content.¹⁹

Generally the pornography regulated in Indonesia refer to the Information Technology and Electronic Transaction and its amendments, Pornography law, and The Right to Be Forgotten for victims of Online-based Sexual Violence has been guaranteed in Article 70 paragraph (2) letter 1 of the Law on Sexual Violence Crimes. Therefore, for regarding of Online-based Sexual Violence has to be analyze further to determain the congcrate legal base.



Source: A deepfake app advertised itself on Meta platforms using faces of actors Emma Watson (NBC News)

On the other hand, this case also happened in the United Kingdom. In a Facebook ad, a woman with a face identical to actor Emma Watson’s face smiles coyly and bends down in front of the camera, appearing to initiate a

¹⁹ Kumparan News. “Awal Mula Mahasiswa Unud Pembuat Konten Porno ‘Deepfake’ Minta Maaf di Media.” *Kumparan*. April 29, 2025. <https://kumparan.com/kumparannews/awal-mula-mahasiswa-unud-pembuat-konten-porno-deepfake-minta-maaf-di-media-24PYIVIIWCA>. Accessed August 25, 2025.

sexual act. But the woman isn't Watson, the "Harry Potter" star. The ad was part of a massive campaign this week for a deepfake app, which allows users to swap any face into any video of their choosing. Deepfakes are content where faces or sounds are switched out or manipulated. Commonly, deepfake creators make videos in which celebrities are made to look like they are willingly appearing in them, even though they are not. Increasingly, the technology has been used to make nonconsensual pornography featuring the faces of celebrities, influencers or any person, including children.²⁰

The ad campaign on Meta nods to the fact that this once-advanced technology has rapidly spread to readily available consumer applications being advertised on mainstream parts of the internet. Despite many platforms prohibiting manipulative and malicious deepfake content, apps like the ones reviewed by NBC News have been able to slip through the cracks. On Sunday and Monday, an app for creating "DeepFake FaceSwap" videos rolled out more than 230 ads on Meta's services, including Facebook, Instagram and Messenger, according to a review of Meta's ad library. Some of the ads showed what looked like the beginning of pornographic videos with the well-known sound of the porn platform Pornhub's intro track playing. Seconds in, the women's faces were swapped with those of famous actors. When Lauren Barton, a journalism student in Tennessee, saw the same ad on a separate application, she was shocked enough to screen-record it and tweet it out, where it received over 10 million views, according to Twitter's views counter. Of the

²⁰ Kat Tenbarga and Steven Romo, "Emma Watson, Scarlett Johansson Appear in Sexually Suggestive Deepfake Ads Against Their Will," *NBC News*, March 8, 2023, video, accessed August 21, 2025, <https://www.nbcnews.com/now/video/emma-watson-scarlett-johansson-appear-in-sexually-suggestive-deepfake-ads-against-their-will-164749893736>

Meta ads, 127 featured Watson’s likeness. Another 74 featured the actor Scarlett Johansson’s face swapped with those of women in similarly provocative videos. Neither actor responded to a request for comment. “Replace face with anyone,” the captions on 80 of the ads read. “Enjoy yourself with AI swap face technology.”²¹

On Tuesday, after NBC News asked Meta for comment, all of the app’s ads were removed from Meta’s services. While no sexual acts were shown in the videos, their suggestive nature illustrates how the application can potentially be used to generate faked sexual content. The app allows users to upload videos to manipulate and also includes dozens of video templates, many of which appear to be taken from TikTok and similar social media platforms.²²

The terms of service for the app, which costs \$8 per week, say it does not allow users to impersonate others via their services or upload sexually explicit content. The app developer listed on the App Store is called Ufoto Limited, owned by a Chinese parent company, Wondershare. Neither company responded to a request for comment. Meta banned most deepfake content in 2020, and the company prohibits adult content in ads, including nudity, depictions of people in explicit or suggestive positions, or activities that are sexually provocative.²³

“Our policies prohibit adult content regardless of whether it is generated by AI or not, and we have restricted this Page from advertising on our platform,” a Meta spokesperson said in a statement. The same ads were also

²¹ *Ibid*

²² *Ibid*

²³ *Ibid*

spotted on free photo-editing and gaming apps downloaded from Apple's App Store, where the app first appeared in 2022 for free for ages 9 and up. An Apple representative said that the company does not have specific rules about deepfakes but that it prohibits apps that include pornography and defamatory content. Apple said it removed the app from the App Store after having been contacted by NBC News. The app was also previously available to download for free on Google Play, where it was rated "Teen" for "suggestive themes." Google said Wednesday it removed the app from Google Play after having been contacted by NBC News. Apple and Google have taken action against similar AI face-swap apps, including a different app that was the subject of a Reuters investigation in December 2021. Reuters found that the app was advertising the creation of "deepfake porn" on pornographic websites. At the time, Apple said it didn't have specific guidelines around deepfake apps but prohibited content that was defamatory, discriminatory or likely to intimidate, humiliate or harm anyone. While its ratings and ad campaigns have been adjusted, the app that Reuters reported on is still available to download free on Apple's App Store and Google Play.²⁴

The app NBC News reviewed is one of the latest in a boom of freely accessible consumer deepfake products. When searching "deepfake" on app stores, dozens of apps with similar technological capabilities appear, including ones that promote making "hot" content.²⁵ In addition, in the context of the Sexual Offenses Act, the scope of the term 'movie' includes data stored in any

²⁴ *Ibid*

²⁵ *Ibid*

way that can be converted into a video of a person's genitals. This could potentially apply to code used to train artificial intelligence systems to generate such content within the scope of the law.²⁶

This study has a number of advantages that make it relevant both theoretically and practically. By highlighting online sexual violence crimes through the phenomenon of deepfakes, this study broadens the scope of criminal law discussions, which previously focused more on conventional cybercrimes. From a theoretical perspective, this research enriches our understanding of the relationship between the development of artificial intelligence technology and criminal law. This analysis is important to strengthen the theory of criminal liability, especially in cases where perpetrators use technology to conceal their identity or create fake pornographic content.

Thus, this research helps fill the gap in scientific studies related to online-based sexual violence. From a practical standpoint, this study offers concrete input for policymakers in Indonesia. By using a comparative legal approach with the United Kingdom, whose regulations are more progressive through the Online Safety Act 2023, this study can provide recommendations that are oriented towards protecting victims while also emphasizing the criminal responsibility of perpetrators. From a social urgency perspective, this research has strategic value because deepfake-based crimes are increasingly prevalent and cause psychological, social, and reputational harm to victims,

²⁶ Bullyid Indonesia, "Perbandingan Hukum Deepfake di Berbagai Negara," *Bullyid Indonesia*, June 20, 2024, <https://bullyid.org/educational-resources/perbandingan-hukum-deepfake/>

especially women. With the increasing use of digital technology in Indonesia, the risk of deepfake-based pornography is getting higher, so a clear and comprehensive legal framework is needed. Therefore, this research is an academic effort to respond to the public's need for adequate legal protection in the digital era.

The United Kingdom was chosen as a comparison country because it already has relatively advanced and comprehensive regulations governing technology-based crimes, especially those related to deepfake-based pornography. This is reflected in the Online Safety Act 2023, which explicitly regulates the obligation of digital platforms to remove non-consensual sexual content, including deepfake pornography, and confirms the forms of criminal sanctions through Sections 66A and 66B.

In addition, the United Kingdom is among the more progressive countries in adapting criminal law to developments in information technology, unlike Indonesia, which still uses the Electronic Information and Transactions Law, the Pornography Law, and the Law on Sexual Violence Crimes partially to construct the offense of deepfake-based pornography. Thus, a comparison with the United Kingdom can provide a clearer picture of modern regulations, sanctions, and victim protection that can be used as a reference for legal reform in Indonesia.

B. Problem Formulations

1. How is the comparison regarding the criminal offences related to deepfake-based pornography as sexual violence in Indonesia and United Kingdom?
2. How is the comparison regarding the sanctions related to deepfake-based pornography as sexual violence in Indonesia and United Kingdom?

C. Research of Method

This research employs a normative juridical method using a comparative legal approach. Primary legal materials include statutory regulations and case law, which are supported by secondary sources such as books, journals, and academic articles, and tertiary sources such as legal dictionaries and encyclopedias. Data were gathered from literature and document studies and analyzed qualitatively using descriptive and comparative methods. This research aims to analyze the differences in legal regulations concerning deepfake-based pornography between Indonesia and the United Kingdom, focusing on how each country addresses Online Sexual Violence (OSV). By comparing the regulations and the sanctions imposed on violators, this study seeks to understand the effectiveness and scope of existing laws in both jurisdictions related to deepfake-based pornography.

D. Originality of The Study

Previous research refers to findings or results from previous studies that are used by researchers as a reference or basis for their research and writing. Previous research is helpful in providing insight into similar issues in

other regions and for enriching the material studied in this research. However, limited research has been conducted on a direct comparative analysis of Indonesia and the United Kingdom's legal frameworks concerning deepfake-based pornography. The following is a description of previous research conducted by researchers.

The first one is from Koopman, M., et al. (2022) "*Regulating Deepfake Technology in Criminal Law: Challenges and Opportunities*".²⁷ This research explores the global legal responses to deepfake technology, with a focus on how different legal systems address deepfake-based crimes. While it provides an overview of regulations in several countries, including the UK, it does not specifically compare Indonesia's legal framework. Comparison between this and Koopman's research by narrowing its focus to deepfake pornography and online sexual violence, offering a more in-depth analysis of specific legislative provisions and their effectiveness in practice.

From Castellanos Saavedra, C. (2024). "*Criminalizing Deception: A comparative analysis on the legislation of the United Kingdom and the Netherlands targeting Deepfake Non-Consensual pornography*".²⁸ Cristina Castellanos Saavedra's research has indeed discussed non-consensual deepfake pornography by comparing the United Kingdom and the Netherlands, particularly in terms of regulatory weaknesses, cross-border jurisdiction, and

²⁷ Marissa Koopman et al., "Detection of Deepfake Video Manipulation," in *Proceedings of the 20th Irish Machine Vision and Image Processing Conference* (2018)

²⁸ C. Castellanos Saavedra, *Criminalizing Deception: A Comparative Analysis on the Legislation of the United Kingdom and the Netherlands Targeting Deepfake Non-Consensual Pornography* (By Maastricht University & A. Giannini, 2024), <https://doi.org/10.13140/RG.2.2.15334.02882>

its connection to image-based sexual abuse in Europe. However, this research is different because it focuses on Indonesia and the United Kingdom, adding analysis that goes beyond regulations and sanctions. Therefore, it brings originality by expanding the study outside the European context, especially in Indonesia, where awareness is still lacking, while emphasizing the dimensions of victim protection and access to justice, which have not been widely discussed in previous studies.

Another previous study, such as Puteri Nurul Izzah's (2024) thesis with "*Analisis Yuridis Manipulasi Gambar Deepfake Pornografi*".²⁹ The mainly examined deepfake pornography in the context of Indonesian law, framing it as a form of forgery and concentrating on doctrinal interpretations of criminal liability. While such research is useful in clarifying the legal definition of deepfake manipulation, it is limited to a single jurisdiction and does not consider broader comparative perspectives with this study providing a comparative legal analysis between Indonesia and the United Kingdom.

E. Literature Review

This section will discuss the theories used in this research proposal, which were derived from laws, literature and journals.

1. Crimes of Pornography

a. Pornography Law

When referring to the Pornography Law, the abuse of deepfake porn is included in the elements stipulated in Article 1 number 1 of the

²⁹ Puteri Nurul Izzah, "Analisis Yuridis Manipulasi Gambar Deepfake Pornografi" (Thesis, Universitas Islam Negeri Sunan Ampel Surabaya, 2024).

Pornography Law as follows:³⁰ Pornography is images, sketches, illustrations, photographs, writings, sounds, moving images, animations, cartoons, conversations, gestures, or other forms of messages through various forms of communication media and/or public performances, which contain obscenity or sexual exploitation that violates the norms of decency in society. Article 4 paragraph (1) of the Pornography Law prohibits every person from producing, making, reproducing, duplicating, disseminating, broadcasting, importing, exporting, offering, trading, renting, or providing pornography that explicitly contains:

- 1) *Intimacy, including deviant intimacy;*
- 2) *Sexual violence;*
- 3) *Masturbation or jacking off;*
- 4) *Nudity or the appearance of nudity;*
- 5) *Genitals; or*
- 6) *Child pornography.*³¹

Then, perpetrators who violate the prohibition in Article 4 paragraph (1) of the Pornography Law can be punished with imprisonment for a minimum of 6 months and a maximum of 12 years and/or a fine of at least IDR 250 million and a maximum of IDR 6 billion, as stipulated in Article 29 of the Pornography Law.³²

³⁰ Article 1 (1) of Law Number 44 of 2008, pornography is defined broadly to include various media and forms of sexual content (Art. 1(1))

³¹ Article 4 (1) of Law Number 44 of 2008 prohibits the creation and distribution of pornographic content containing explicit sexual material

³² Article 29 of the Pornography Law stipulates sanctions ranging from 6 months to 12 years in prison and fines up to IDR 6 billion for those violating Article 4 (1)

b. Electronic Information and Transaction Law

Electronic Information and Transaction Law or ITE Law for short defined as a law that regulates a number of information activities and electronic transactions in the digital world. A number of rules written in the Electronic Information and Transaction Law aim to monitor and protect activities on the internet. More specifically, to keep the digital space healthy, clean, productive, and obedient to certain ethics. The clean and healthy referred to in the scope of the Electronic Information and Transaction Law also includes various legal bases for the use of technology. That way, acts of online crime or cyber crime can have a legal basis.

Electronic Information and Transaction Law regulates various things so that users of information technology and electronic transactions can get legal certainty. That way, the most important benefit of Electronic Information and Transaction Law is to provide legal protection for users of digital space. Legal certainty from Electronic Information and Transaction Law is useful for increasing the trust of technology users. Everyone can finally access the technology without having to worry about security, for example in electronic transactions. In this regard, the Electronic Information and Transaction Law provides legal certainty. A number of Electronic Information and Transaction Law rules regulate this, such as tapping, fraud and others.³³

³³ Heinrich, R. (2024c, September 25). *Memahami UU ITE: Dasar hukum, manfaat, dan sanksi pelanggaran*. Hukumku. <https://www.hukumku.id/post/memahami-uu-ite>

c. Sexual Violence Crimes

According to Simos, a crime is a human act that is against the law. Which actions are carried out by someone who is accountable, can be hinted at by the perpetrator or the perpetrator.³⁴ Meanwhile, Moeljatno uses the term criminal act which is defined as an act that is prohibited by law, where the prohibition is accompanied by threats of sanctions which can be in the form of certain crimes, for anyone who carries out the prohibition. Then, according to Andi Hamzah uses the term offense which is defined as an act or action prohibited and threatened with law by law.³⁵ The term violence, in the Indonesian Dictionary (KBBI), has the meaning of something that has a violent nature or the existence of coercion in an act of a person or group of people that causes physical damage or an object.³⁶ Literally, violence is a form of action that is more physical in nature, which can cause injury, disability, illness, or suffering to other people, where there is an element of coercion or unwillingness or lack of approval from other people.³⁷ Violence is an action that leads to behavior that initially must be contrary to the law, either only in the form of threats or in the form of real actions and causes damage to property, physical or can result in death of someone.³⁸ Yesmil Anwar defines violence as an act that uses physical strength and power, threats

³⁴ C.S.T. Kansil, 2001, Criminal Law Examination Training, Jakarta: Sinar Graphic, p.106.

³⁵ C.S.T. Kansil and Christine S.T. Kansil, 2004, Fundamentals of Criminal Law, Jakarta: Pradnya Paramita, p. 54.

³⁶ Indonesia Dictionary.

³⁷ Abdul Wahid and Muhammad Irfan. 2001, Protection of Victims of Sexual Violence: Advocacy for Women's Human Rights. Bandung: Refika Aditama. p. 54

³⁸ Romli Atmasasmitha, Theory & Capita Selektu Criminology, PT. Eresco, Bandung, 1992, p.55.

or actions against oneself, an individual, a group of people or society which results in bruising or trauma, death, psychological harm, developmental disorders and deprivation of rights.³⁹ Sexual violence tends to have a traumatic impact on victims. However, cases of sexual violence often go unresolved due to denial of the incidents of sexual violence that occurred. Victims of sexual violence tend not to trust other people, so they keep the incidents of sexual violence secret. In addition, victims are afraid to report perpetrators because they feel threatened that they will experience worse things if they report, and feel ashamed because the events they are experiencing can damage their family name.⁴⁰ Under the Law on Sexual Violence Crimes, sexual harassment is a form of sexual violence that consists of physical sexual harassment and non-physical sexual harassment,⁴¹ as follows:

1) Non-physical sexual harassment is a non-physical sexual act directed against the body, sexual desires, and/or reproductive organs with the intention of degrading a person's dignity based on their sexuality and/or morality.⁴² Examples of non-physical sexual acts are inappropriate statements, gestures, or activities that lead to sexuality with the aim of degrading or humiliating.

2) Physical sexual harassment consists of three forms namely:⁴³

³⁹ Yesmil Anwar, *Reaping Crime: A Sociocultural Approach to Criminology, Law and Human Rights*, UNPAD Press, Bandung, 2004, p. 54.

⁴⁰ Ivo Noviana, 2015, *Sexual Violence Against Children: Its Impact and Handling*, *Journal of Sosio Informa*, Vol. 01, No. 1, p. 18.

⁴¹ Article 4 paragraph (1) letters a and b of Law Number 12 Year 2022 on the Law on Sexual Violence Crimes

⁴² Indonesian Law No. 12 of 2022 on Law on Sexual Violence Crimes, Article 5

⁴³ Indonesian Law No. 12 of 2022 on Law on Sexual Violence Crimes, Article 6

- a) Physical sexual acts directed against the body, sexual desires, and/or reproductive organs with the intention of degrading a person's dignity based on their sexuality and/or morality.
- b) Physical sexual acts directed against the body, sexual desires, and/or reproductive organs with the intention of unlawfully placing someone under their power, both inside and outside of marriage.
- c) Abuse of power, authority, belief, or influence arising from deception or a relationship of circumstances or taking advantage of a person's vulnerability, inequality or dependency, forcing or misleadingly leading that person to commit or tolerate sexual intercourse or obscene acts with him or someone else.

2. Online Sexual Violence (OSV)

According to Veryanto Sitohang, as Komnas Perempuan commissioner explained nine forms of online sexual violence including:⁴⁴

1) Cyber Hacking

Cyber hacking is a form of action or business that uses the internet to access data illegally, secretly, or without the data owner's permission. The data is obtained for use or modification. In the context of Online Gender Based Violence (OGBV), hacking or hacking is an attempt made so that the perpetrator can access the victim's data, such as photos, videos,

⁴⁴ Puti Malya, 9 Types of Violence against Women on the Internet, One of which is Sexting, found in <https://www.parapuan.co/read/532930269/9-jenis-kekerasan-pada-perempuan-di-internet-salah-satunya-sexting?page=all>, accessed on Wednesday, July 26th 2023, at 22.32 WIB.

or other valuable documents. Perpetrators can also take over someone's social media account without permission.

2) Impersonation

Impersonation is an activity using technology to assume the victim's or someone else's identity to access private information, embarrass or shame the victim, contact the victim, or create fraudulent identity documents.

3) Cyber Surveillance

Cyber Surveillance has another name, such as; Stalking and Tracking. Cyber Surveillance uses technology to stalk and monitor a victim's activities and behaviours in real-time or historically. Stalking involves repeated incidents, which may be harmless. However, the combined acts can undermine the victim's sense of security and cause distress, fear or intimidation.

4) Cyber harassment

Cyber harassment is using the internet to threaten, intimidate, or shame an individual. The methods include threats, stalking, insults, and spreading private information to others. Sexual harassment in online settings can be categorized as cyber harassment.

5) Cyber Recruitment

Cyber recruitment uses technology to manipulate victims so they are lured into adverse and dangerous situations. Usually, victims are contacted online and lured with job opportunities. The perpetrators use this mode to gather victims' data and spread their videos/photos in online forums.

6) Malicious Distribution

The use of technology to spread content that can damage the victim's reputation regardless of the truth. Much like the NonConsensual Dissemination of Intimate Images (NCII). The perpetrator usually threatens to share the victim's photos or videos. The difference is that the shared content is not limited to intimate content.

7) Non-Consensual Dissemination of Intimate Image (NCII)

Non-Consensual Dissemination of Intimate Images (NCII) or better known by its problematic term "revenge pornography", is the act of distributing images or videos online without the consent of one or more people involved in the images or videos.

8) Sexting

In his book entitled "Sexting Gender and Teens", Judith Davidson explains that sexting is the activity of sending sexually explicit messages or images or highlighting sexual material through technological products connected to the internet (in this case, smartphones).

9) Morphing

They create synthetic/fake/artificial sexual images to place someone's face over a sexually imaged body.

3. Criminal Penalties

Criminal penalties are the legal consequences imposed by a court on individuals who have been convicted of crimes. These penalties can include

imprisonment, fines, community service, probation, and other forms of punishment intended to deter criminal behavior, rehabilitate offenders, and provide restitution to victims. Different types of crimes can result in varying degrees of penalties based on the severity of the offense and the impact on society.⁴⁵ The forms of criminal penalties in Indonesian positive law are divided into two, namely (1) basic punishment, which is in the form of death penalty, imprisonment, confinement, fines, and closure; and (2) additional punishment, which is in the form of revocation of certain rights, seizure of property, and judges' verdict declaration.⁴⁶

F. Definition Of Term

1. DeepFake

“Deepfakes” can be defined as the use of Artificial Intelligence (AI) techniques (such as machine and deep learning and, more specifically, Generative Adversarial Networks) to generate synthetic but exceedingly realistic video and audio media, especially of human facial and vocal likeness.⁴⁷ Deepfake is an Artificial Intelligence (AI) technology used to manipulate images and videos by fusing a person's face onto another person's body. This creates a very realistic representation, including in the context of pornography without the consent of the original subject. Deepfake pornography focuses on using Artificial Intelligence (AI)

⁴⁵ *Criminal penalties - (Criminal Law) - Vocab, Definition, Explanations | Fiveable.* (n.d.). <https://library.fiveable.me/key-terms/criminal-law/criminal-penalties>

⁴⁶ Article 10 of the Criminal Code.

⁴⁷ Chesney, R., & Citron, D. (2019). *Deepfakes: A looming challenge for privacy, democracy, and national security.* *California Law Review*, 107(6), 1753–1820. <https://doi.org/10.15779/Z38RV0D15J>

technology to produce content that appears authentic, but is actually the result of digital engineering. Deepfake technology allows for the manipulation of a person's face so that it can resemble that of another person, whether in video or photo form. Over time, the quality of content produced by deepfakes has improved. As manipulation techniques become more complex, it becomes more challenging to determine whether a video or photo is real or the result of deepfake technology. Deepfakes have great potential to quickly damage a person's reputation, as many individuals misuse these applications to spread negative content, such as fake news, data manipulation, and sexual or pornographic material. Easy access to this technology is often utilized in unethical ways, especially in creating deepfakes without the permission of the data owner. This can lead to negative impacts for victims, especially when deepfakes are used to produce harmful pornographic content, exposing them to significant legal risks.⁴⁸

2. Pornography

Pornography means the portrayal of erotic acts through paintings or writing to provoke sexual desire.⁴⁹ Pornography is images, sketches, illustrations, photographs, writings, sounds, moving images, animations, cartoons, conversations, gestures, or other forms of messages through various forms of communication media and/or public performances, which contain obscenity or sexual exploitation that violates the norms of decency

⁴⁸ Wicaksana, F., & Yuli, Y. (2024). *Legal Protection for Victims of Deepfake Porn Abuse In The National Criminal Law System* (Vol. 8, Issue 3).

⁴⁹ Departemen Pendidikan Nasional, "Kamus Besar Bahasa Indonesia", edisi III (Jakarta: Balai Pustaka, 2005), p.889

in society. Pornographic services are all types of pornographic services provided by individuals or corporations through live performances, cable television, terrestrial television, radio, telephone, internet, and other electronic communications as well as newspapers, magazines, and other printed matter.⁵⁰

3. Criminal Policy

Criminal politics is often known as criminal policy. There are various opinions that explain this concept. However, in short, criminal politics is a concept formed to protect society or to achieve public welfare. Sudarto defines criminal politics as a rational and organized effort of a society to overcome crime. Barda Nawawi Arief explained that definition was abstracted from the understanding formulated by Marc Ancel. Marc Ancel formulated it as the rational organization of the control of crime by society, which when translated means the rational organization of crime control by society.⁵¹

Marc Ancel put forward the definition of criminal policy by stating that “*The national organization of the control of the crime by society*”. Departing from this definition, G. Peter Hoefnagels argued that, “*criminal policy is the rational organization of the social reaction to crime.*” Furthermore, he stated that criminal policy can be explained as follows:⁵²

⁵⁰ Law of the Republic of Indonesia Number 44 of 2008 on Pornography.

⁵¹ Pengertian Kebijakan Kriminal (Criminal Policy)," *Digilib Universitas Lampung*, accessed on 26 May 2025, <http://digilib.unila.ac.id/10025/4/BAB%20II.pdf>.

⁵² Hukumonline, “Politik Kriminal dan Politik Hukum Pidana,” *Hukumonline*, April 15, 2022, <https://www.hukumonline.com/berita/a/politik-kriminal-dan-politik-hukum-pidana-lt6258f7d33c289/>.

- a. Criminal policy is the science of response
- b. Criminal policy is the science of crime prevention
- c. Criminal policy is a policy of designating human behavior as crime
- d. Criminal policy is a rational total of the responses to crime

G. Research Method

This research would be conducted with the specifications as follow:

1. Type of Research

The author uses normative research methods. Normative research is a legal research method conducted using literature or legal document studies because this research places limits only on written regulations or other legal materials.⁵³

2. Data Source

Primary legal materials; in this research are binding legal sources consisting of basic norms or rules, laws and regulations and court decisions. Primary legal materials used in this research are:

1. Law Number 44 of 2008 concerning Pornography (Indonesia).
2. Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), amended by Law Number 19 of 2016 and Law Number 1 of 2024.
3. Law Number 12 of 2022 concerning Law on Sexual Violence Crimes (TPKS Law).

⁵³ Soerjono Soekamto dan Sri Mamuji, *Penelitian Hukum Normatif*, Cetakan ke-9, PT Raja Grafindo Persada, Jakarta, 2004, 14.

4. Criminal Code (KUHP) Indonesia

5. United Kingdom, Online Safety Act 2023.

Secondary Legal Materials; in this research are legal materials that use regulations that are used as support and provide explanations for primary legal materials, both in the form of theories as basic principles and legal interpretations or opinions. Secondary legal materials are data obtained from library materials. Secondary legal materials used by the author in this study are:

- a. Books related to the research
- b. Research results of scientific papers, journals and other articles related to the research.
- c. Internet sites that can be accounted for and have a relation to the research focus.

Tertiary Legal Materials in this research are legal materials that are complementary to the existence of primary legal materials and secondary legal materials.

- a. English Dictionary
- b. Legal Dictionary

3. Method of Collecting Legal Materials

This research applies library research, namely collecting and examining legal materials from statutory regulations, books, journals, and other relevant documents.

4. Data Analysis Method

The analysis is conducted using a qualitative descriptive method, by interpreting, comparing, and discussing legal materials to provide answers to the research problems.

H. Research Outlines

The preparation of this research is carried out with a writing systematic consists of four chapters as follows:

CHAPTER I INTRODUCTION

CHAPTER I contains: Background, Problem Formulations, Research Objectives, Literature Review, Definition of Term, and The Legal Method Research.

CHAPTER II OVERVIEW

CHAPTER II General Overview which contains and discusses explanations of theories, research results, and expert opinions about the focus of research. It should be noted that the General Review is not a collection of existing theories, but rather theories that are relevant and appropriate to the research conducted in order to support the research, a theoretical framework is needed as stated by Ronny H Soemitro that to provide a solid foundation in general, every research must be accompanied by theoretical thinking. (Ronny Hanitijo Soemitro, Methodology, Op.Cit, p. 37.) In this case it is explained about: Overview of Deepfake Pornography, The regulations and the sanction between Indonesia and United Kingdom.

CHAPTER III ANALYSIS AND DISCUSSION

CHAPTER III contains the results of research analysis and discussion of the regulation and sanction arrangements governing deepfake pornography in Indonesia and United Kingdom.

CHAPTER IV CONCLUSION AND SUGGESTION

CHAPTER IV is a closing that contains conclusions and suggestions in accordance with the formulation of the problem.