Legal Protection for Victims of Artificial Intelligence Misuse in the Form of **Deepfake Technology**

Gregorius Widiartana¹ Ebenhaezar Parlindungan Lumbanraja²

Faculty of Law, Universitas Atma Jaya Yogyakarta, Sleman, Special Region of Yogyakarta, Indonesia^{1,2}

Email: g.widiartana@uajy.ac.id1 ebenhaezarlumbanraja@gmail.com2

Abstract

The development of technology has reached the Fourth Industrial Revolution, marked by the integration of information technology into the industrial world. In this era, information technology plays a crucial role in human daily activities, including the presence of artificial intelligence as a tool to assist human activities in the digital age. Artificial intelligence is like a double-edged sword—it can help humans fulfill their needs, but on the other hand, it can also harm them if misused. One form of artificial intelligence misuse is through deepfake technology. This AI-driven technology, which can manipulate a person's facial visuals in both video and photo formats, is increasingly being exploited by irresponsible parties. This article discusses legal protection for victims of deepfake misuse, focusing on regulations, resolution mechanisms, and the right to be forgotten. This research employs a normative legal research method with a conceptual approach. The findings of this study indicate that legal protection for victims of deepfake misuse can be achieved through strengthening regulations on AI usage, adopting a restorative justice approach for victims, and ensuring the right to be forgotten to safeguard their **online** reputation. Keywords: Deepfake, Victim, Protection



This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

INTRODUCTION

The development of technology in the 4.0 era has brought about a major transformation in human life, changing the way we engage in activities, work, and interact. In this era, information technology and artificial intelligence have made various human activities easier, ranging from business processes to daily life, which can now be carried out more efficiently and practically through online platforms. Activities that were once conventional, such as shopping, working, or learning, can now be done easily through digital devices. This technology not only replaces more manual conventional methods but also creates new, more modern ways that are globally connected, enabling access to information, transactions, and services without limitations of time and place. This accelerates the process of digitization, which increasingly dominates various aspects of life (Abidin, 2015).

One of the manifestations of the 4.0 information technology development that is widely discussed is artificial intelligence (AI), which has a significant positive impact on human activities. AI enables the automation of processes that previously required direct human involvement, improving efficiency and accuracy in various fields, from industry to healthcare and education. In the business world, AI helps in making smarter and faster decisions through complex data analysis, while in healthcare, AI is used to diagnose diseases more accurately and design more precise treatments. Additionally, artificial intelligence plays a role in enhancing user experiences in various applications, such as virtual assistants, recommendation systems, and content personalization, making human life more connected, practical, and productive in this digital era (Saputra, 2018)

Although artificial intelligence (AI) brings many positive impacts, this technology can also have negative consequences if misused, one of which is in deepfake technology. Deepfake uses AI to manipulate images or videos, creating highly realistic yet entirely fake content, such as disguising a person's identity or spreading misleading information. The misuse of this technology can damage an individual's reputation, cause financial loss, and even trigger social and political conflicts. Due to its ability to generate content that is difficult to distinguish from reality, deepfake can be exploited for fraudulent purposes, defamation, or manipulating public opinion, ultimately harming many parties and creating distrust in society (Novyanti, 2021).

One example of a deepfake technology misuse case that gained significant attention involves public figure Nagita Slavina, an Indonesian celebrity. In this case, a deepfake video using Nagita Slavina's face was circulated on social media, causing distress as the content presented a false image that harmed her personal and professional reputation. This case highlights how deepfake can be used to spread misleading information and damage someone's image without consent, as well as the legal challenges faced in addressing such misuse of technology (Mutmainnah et al., 2024). Legal protection for victims of deepfake like this becomes increasingly important to prevent harmful impacts in the digital world.

In Indonesia, the misuse of deepfake technology can be prosecuted under several regulations in laws, one of which is the Electronic Information and Transactions Law (UU ITE) No. 19 of 2016, which regulates defamation, the spread of false information, and fraud through electronic media. In the case of deepfake misuse, if the technology is used to defame or spread false information that harms individuals or groups, the perpetrator may face criminal penalties. Additionally, the perpetrator can also be prosecuted under the Personal Data Protection Law (UU PDP) No. 27 of 2022, which protects personal data and an individual's privacy from unauthorized use, including in the context of manipulating someone's face or identity through deepfake. These regulations provide a legal basis for addressing the misuse of deepfake technology and offer protection for victims.

Although Indonesia has several regulations that can be used to prosecute perpetrators of deepfake misuse, the existing laws are still considered inadequate to resolve cases thoroughly. These regulations mostly focus on criminal sanctions that can be imposed on deepfake technology abusers, such as those outlined in the ITE Law and the Personal Data Protection Law. However, these regulations have yet to provide adequate protection for victims, both in terms of reputation recovery and other rights that may be violated. Deepfake victims still do not have guarantees to request the removal of harmful content or obtain compensation for the damages caused. Furthermore, law enforcement against deepfake perpetrators is also hindered by technical challenges and the difficulty of obtaining evidence (Laza & Karo Karo, 2023) Therefore, strengthening regulations is needed, not only focusing on sanctions but also on victim protection and more effective law enforcement.

In addition, it is urgent to protect the right to be forgotten for victims of deepfake misuse, particularly in relation to privacy and reputation in the digital world. As deepfake technology can distort an individual's image and spread false information, it directly impacts their personal privacy and public reputation. The right to be forgotten would allow victims to request the removal of harmful content and prevent its further circulation, helping to restore their dignity and privacy. This right is crucial in the digital age, where online content can have long-lasting and far-reaching consequences. Strengthening legal frameworks that uphold this right can provide necessary safeguards, ensuring that individuals are not permanently harmed by digital manipulations such as deepfakes. This article discusses legal protection for victims of artificial intelligence misuse in the form of deepfake technology. The research focuses on efforts to establish adequate legislation to address victims of deepfake misuse, mechanisms for resolving deepfake-related cases based on restorative justice, and the need to guarantee the right to be forgotten as a form of human rights protection for victims.

RESEARCH METHODS

Normative legal research is a research method that focuses on analyzing legal norms contained in legislation, doctrines, and court decisions to identify applicable legal principles. This type of research is conceptual and theoretical, employing an approach that examines primary and secondary legal materials to provide a comprehensive understanding of the legal norms that should be applied (Sulaiman, 2018). Legal materials are categorized into primary and secondary legal materials. Primary legal materials include legislation, court decisions, and treaties, while secondary legal materials consist of doctrines, legal journals, and expert opinions, which serve as references for understanding and interpreting primary legal materials (Marune, 2023). The technique of collecting legal materials through literature study involves examining various written sources such as legislation, court decisions, books, legal journals, and other official documents. This method aims to establish a strong theoretical foundation for analyzing the legal issues under study (Rifa'i, 2023). The technique of legal material analysis using the deductive method involves drawing conclusions from general legal principles to be applied to specific cases or legal issues. This approach aims to ensure consistency in legal interpretation and to find solutions that align with applicable legal norms (Irianto, 2017)

RESEARCH RESULTS AND DISCUSSION

Deepfake is a form of artificial intelligence that utilizes machine learning technology, particularly deep learning, to manipulate or fabricate images, videos, and audio to closely resemble a specific individual. This technology can be used for various purposes, both positive, such as in the entertainment and education industries, and negative, such as spreading false information, defamation, and privacy violations. In the legal context, the misuse of deepfake poses challenges in regulation and victim protection, highlighting the need for comprehensive policies to address these issues (Gunawan & Janisriwati, 2023). Initially, deepfake technology was developed and utilized in the film industry to enhance visual effects and create more realistic digital characters. This technology allows filmmakers to replace actors' faces, revive deceased characters, or generate scenes without requiring actors to be physically present. With the advancement of deep learning, visual editing processes have become smoother and more natural, providing audiences with a more immersive cinematic experience (Gandrova & Banke, 2023). However, as it evolved, deepfake technology began to be misused beyond the entertainment industry, such as in the creation of fake content, political manipulation, and privacy violations, raising various ethical and legal challenges.

One example of a deepfake case in political propaganda occurred during the 2020 Indian elections, where a deepfake video was used to alter politician Manoj Tiwari's speech so that it could be delivered in multiple languages, reaching a wider audience. Although the initial goal was to expand political campaigning, this technology raised concerns about its potential misuse in spreading disinformation and manipulating public opinion. Additionally, in the United States, deepfake technology has also been utilized in various political propaganda efforts, such as videos depicting political figures making statements they never actually said, potentially damaging reputations and influencing election outcomes (Leliana et al., 2024) This case highlights the urgent need for regulations on the use of deepfake technology in political contexts to prevent its misuse. Aside from propaganda in the political sphere, deepfake is also widely misused for creating fake pornographic content and spreading defamation and hoaxes. One example of deepfake misuse for pornographic content in Indonesia is the case involving celebrity Nagita Slavina. In January 2022, a 61-second video featuring a figure resembling her in an inappropriate scene circulated widely on social media. After an investigation, the police

confirmed that the video was a digitally manipulated creation using deepfake technology, where Nagita Slavina's face was superimposed onto another person's body. This case highlights the dangers of deepfake misuse in generating fake pornographic content, which can damage a person's reputation and violate their privacy. This incident also serves as a warning about the urgent need for stricter regulations and effective legal measures to protect victims from the negative impacts of deepfake technology (Muhammad Rifki Noval, 2019).

Indonesia essentially already has regulations that can be used to address cases of deepfake misuse, particularly through the Electronic Information and Transactions Law (UU ITE). The UU ITE regulates various legal aspects related to the dissemination of information in digital spaces, including provisions on defamation, the distribution of illegal content, and the manipulation of electronic data that may harm individuals or society. In the context of deepfake, the articles within the UU ITE can serve as a legal basis to take action against perpetrators who intentionally spread manipulative content that harms victims, whether in the form of defamation or the dissemination of false information. Articles in the Electronic Information and Transactions Law (UU ITE) that can be used to prosecute perpetrators of deepfake misuse include Article 27(1), which prohibits the distribution of content violating decency, Article 27(3) on defamation, and Article 28(1), which regulates the dissemination of false information that could mislead the public. Additionally, Article 35 of the UU ITE can also be applied in deepfake cases, as it addresses the falsification of electronic information and/or electronic documents with the intent to deceive. Under these provisions, individuals who create or distribute deepfake content with the intent to harm others may face criminal sanctions, including fines or imprisonment, in accordance with the UU ITE regulations.

Although the Electronic Information and Transactions Law (UU ITE) can be used to prosecute perpetrators of deepfake misuse, several weaknesses make law enforcement less effective. One of the main weaknesses is the absence of specific provisions regulating deepfake as a form of artificial intelligence-based digital manipulation. As a result, existing articles, such as Article 27 and Article 28, are often interpreted broadly, leading to legal uncertainty in their application. Moreover, the UU ITE focuses more on the distribution of illegal content rather than its creation. This makes it difficult to prosecute individuals who merely create deepfake content without directly distributing it. The lack of regulations governing the responsibility of digital platforms in handling deepfake content is another weakness, considering that the spread of deepfake videos often occurs through social media and video-sharing sites. Another issue is that the penalties stipulated in the UU ITE are still considered insufficient to deter deepfake misuse. The punishments prescribed in the law tend to be relatively lenient compared to the severe consequences that deepfake content can cause, such as defamation, reputational damage, or the spread of misinformation that may lead to social instability. Therefore, revisions and adjustments to the UU ITE are necessary to make it more relevant in addressing emerging challenges posed by deepfake technology.

In addition to the provisions in the UU ITE, the regulations in Law Number 44 of 2008 on Pornography can also be used to prosecute perpetrators of deepfake misuse, especially if the created or distributed content contains pornographic elements. Article 4(1) of the Pornography Law prohibits the creation, distribution, and use of pornographic content in any form, including those generated using digital technology such as deepfake. Furthermore, Article 29 of the Pornography Law stipulates criminal penalties for anyone who produces, distributes, or facilitates access to pornographic content illegally. With these provisions in place, individuals who create or distribute fake pornographic deepfake content can face stricter legal consequences, including imprisonment and fines, to protect victims and prevent the misuse of technology in the digital space.

Although Law Number 44 of 2008 on Pornography can be used to prosecute perpetrators of deepfake misuse, several weaknesses make its enforcement less effective. One of the main weaknesses is that the definition of pornography in this law still focuses on conventionally created content, such as real images, writings, or videos, without explicitly covering digitally manipulated content generated by artificial intelligence, such as deepfake. As a result, the legal enforcement of deepfake pornography relies on varying legal interpretations, leading to uncertainty in applying sanctions against offenders. Additionally, the Pornography Law primarily emphasizes the production, distribution, and consumption of pornographic content without specifically addressing digital manipulation acts such as deepfake. This makes it difficult to prosecute individuals who merely create deepfake pornography without distributing it, even though such content can be used to harm victims. Moreover, the absence of clear regulations regarding the responsibility of digital platforms in filtering and removing deepfake pornographic content makes its spread even harder to control, particularly on social media and video-sharing platforms with a broad audience.

Another weakness is that the sanctions outlined in the Pornography Law are still limited in providing a strong deterrent effect against deepfake pornography perpetrators. The penalties in this law are more oriented toward traditional forms of sexual exploitation and have yet to fully address new violations arising from technological advancements. Therefore, revisions to the Pornography Law are necessary to make it more relevant in addressing new challenges, including the misuse of deepfake technology in the creation and distribution of pornographic content that harms individuals and society. The development of artificial intelligence technology, particularly deepfake, has introduced new challenges in legal and ethical aspects. Although Indonesia has various positive legal regulations, such as the Electronic Information and Transactions Law (UU ITE) and the Pornography Law, these regulations still have weaknesses in comprehensively addressing the misuse of deepfake technology. The lack of clear definitions in existing laws creates legal uncertainty in prosecuting perpetrators who exploit this technology to harm individuals or society. Therefore, a more robust legal framework is needed to accommodate the deepfake phenomenon and the broader development of artificial intelligence.

One of the main weaknesses of existing laws is the absence of specific provisions regulating deepfake as a form of AI-based digital manipulation. The UU ITE, for example, focuses only on the dissemination of false or illegal information without explicitly addressing the process of creating deepfake content itself. This makes it difficult to prosecute perpetrators who merely generate deepfake content but do not distribute it directly. Similarly, the Pornography Law primarily focuses on explicit content in conventional forms, without including AI-generated content such as deepfake within its regulatory scope. Furthermore, the current legal framework is not sufficiently adaptive to the rapid advancements in technology. Deepfake is not only used for pornography or defamation but also in politics, financial fraud, and information manipulation that can disrupt social stability. Existing laws have yet to clearly define the responsibilities of digital platforms in handling deepfake dissemination, making it difficult to control the spread of such manipulative content. Therefore, a legal approach that is not only repressive but also preventive is necessary, such as requiring digital platforms to implement deepfake detection systems and enhancing digital literacy among the public.

Given the continuously evolving challenges posed by deepfake, a specialized regulation that adapts to AI advancements is crucial. A new law must be capable of addressing various aspects of deepfake misuse, including its creation, distribution, and legal consequences. Additionally, it should establish mechanisms for protecting deepfake victims, including the right to be forgotten, as well as impose stricter sanctions on perpetrators. With a

comprehensive approach, such regulations can ensure that artificial intelligence usage remains within clear ethical and legal boundaries. With the implementation of a more robust and adaptive regulatory framework, Indonesia can be better prepared to tackle legal challenges in the increasingly complex digital era. The law must be able to keep pace with technological advancements without hindering innovation, ensuring individual protection while fostering technological progress. Therefore, concrete steps must be taken in formulating relevant regulations that align with AI developments, preventing deepfake from becoming an increasingly uncontrollable threat.

In addition to drafting a comprehensive law to address the misuse of deepfake technology, the mechanism for resolving deepfake-related cases must also be carefully considered to ensure effective justice for victims. Case resolution should not be limited to imposing legal sanctions on perpetrators but must also be based on the principle of restorative justice. Restorative justice emphasizes victim recovery and rehabilitation while considering the best ways to mitigate the negative impacts caused by deepfake misuse. With this approach, legal proceedings are not only repressive but also provide space for victims to recover from all forms of harm they have suffered. Deepfake victims often experience both material and immaterial losses. In terms of material damage, the dissemination of deepfake content can result in job loss, reputational damage, and financial burdens due to prolonged legal processes. Meanwhile, immaterial losses include psychological effects such as stress, depression, and loss of self-confidence due to digital exploitation. Therefore, the resolution mechanism for deepfake cases must include compensation or restitution for victims, whether in the form of financial reparations or psychological rehabilitation, to help them recover and move forward without long-term distress.

Furthermore, the physical and psychological impact of deepfake misuse should not be overlooked. In cases of deepfake pornography, for instance, victims often suffer from extreme mental distress due to online harassment and the social stigma attached to them. Feelings of shame, fear, and anxiety can have long-term consequences, affecting their social and professional lives. As a result, deepfake case resolutions should include psychological support for victims, provided by the state, in the form of counseling services, therapy, and maximum legal protection. On the other hand, resolving deepfake-related cases should also take corrective measures for perpetrators into account, particularly in terms of education and rehabilitation. Deepfake perpetrators are not always individuals with malicious intent; in some cases, they may simply be exploiting technology without understanding its legal and ethical consequences. Therefore, in addition to strict legal sanctions, an educational approach for perpetrators is crucial to prevent similar cases in the future. Rehabilitation programs for offenders can include training in digital ethics, legal awareness, and the social consequences of technology misuse.

By combining restorative justice, victim recovery, and corrective action for perpetrators, deepfake case resolution can be more effective in providing protection and legal certainty for all parties involved. Strong legal enforcement and comprehensive recovery mechanisms will ensure that deepfake misuse is not only punished but also prevented through education, digital awareness, and better protection for society. Thus, Indonesia's legal system can be better prepared to face new challenges arising from the rapid development of artificial intelligence and digital technology. One of the most crucial aspects of recovery for victims of deepfake misuse is the implementation of the right to be forgotten, as implied in Article 26 of Indonesia's Electronic Information and Transactions Law (UU ITE). This principle grants individuals the right to request the removal of harmful digital information or traces, including deepfake content that has been widely circulated on the internet. In cases of deepfake misuse, victims

often suffer long-term consequences as manipulated content that has already spread becomes difficult to erase completely, continuing to haunt their personal, social, and professional lives. Therefore, enforcing the right to be forgotten is a crucial step in providing protection and recovery for victims.

The implementation mechanism of the right to be forgotten must include clear and effective procedures for victims to request the removal of content. Governments and digital service providers must collaborate to ensure that harmful deepfake content is promptly taken down from digital platforms and search engines. This should not only apply to the original content uploaded but also to any copies that may have been redistributed across various websites or social media platforms. With strict policies and a responsive system in place, victims can be assisted in erasing harmful digital traces that threaten their reputation and wellbeing. Beyond content removal, victim recovery must also include preventive measures to ensure that deleted content does not resurface. In an increasingly sophisticated digital era, data storage and distribution technologies make it possible for erased content to reappear in different formats. Therefore, cooperation between governments, internet service providers, and social media platforms is necessary to ensure that removed deepfake content cannot be easily reuploaded or accessed. Regulations requiring digital platforms to implement monitoring and automated detection systems for deepfake content can be an effective step in preventing further distribution.

However, enforcing the right to be forgotten in deepfake cases still faces numerous challenges, particularly concerning jurisdiction and global policy. The internet operates across borders, meaning that deepfake content deleted in one country may still circulate in another where similar regulations do not exist. Thus, international cooperation is essential in ensuring broader victim protection. Standardizing global policies on digital content removal and fostering intergovernmental collaboration in addressing deepfake cases can enhance the effectiveness of the right to be forgotten in the digital realm. By strengthening the right to be forgotten mechanism, victims of deepfake misuse can receive stronger legal protection and an opportunity to recover from the negative impacts caused. The enforcement of this principle must be accompanied by firm policies, close collaboration between various stakeholders, and public education on digital rights. In doing so, protection for deepfake victims will extend beyond punishing perpetrators, encompassing concrete efforts to eliminate the consequences of harmful content distribution.

CONCLUSION

The rapid advancement of deepfake technology presents both opportunities and significant challenges, particularly in legal and ethical contexts. While deepfake has been used positively in the entertainment and education industries, its misuse for political propaganda, defamation, and pornography raises serious concerns. Existing regulations, such as Indonesia's Electronic Information and Transactions Law (UU ITE) and the Pornography Law, provide a legal basis for prosecuting deepfake-related offenses. However, these laws still lack specific provisions that address deepfake technology comprehensively, creating legal uncertainty and enforcement challenges. One of the key weaknesses in current regulations is their focus on content distribution rather than content creation. This limitation makes it difficult to prosecute individuals who generate deepfake material without directly sharing it. Additionally, the absence of clear accountability for digital platforms further complicates efforts to control the spread of harmful deepfake content. The leniency of existing penalties also fails to serve as an effective deterrent against deepfake misuse, highlighting the need for stricter sanctions and clearer legal definitions to accommodate emerging AI-driven threats. Beyond stricter regulations, deepfake case resolutions must incorporate restorative justice principles to ensure

comprehensive victim protection and rehabilitation. Victims of deepfake misuse often suffer from both material and psychological harm, making legal penalties alone insufficient. Mechanisms such as financial compensation, psychological support, and public awareness campaigns can help mitigate the long-term effects of deepfake-related exploitation. Additionally, rehabilitation programs for offenders, including digital ethics education, can serve as preventive measures against future misuse of the technology. To effectively address deepfake-related challenges, Indonesia must develop a more adaptive and technology-focused legal framework. This includes strengthening the right to be forgotten, enforcing platform accountability, and fostering international cooperation to combat cross-border digital crimes. A balanced approach that ensures legal clarity while promoting AI innovation is crucial to protecting individuals from deepfake misuse. With comprehensive laws and proactive policies, Indonesia can safeguard its digital space while fostering responsible technological advancements.

BIBLIOGRAPHY

- Abidin, D. Z. (2015). Kejahatan dalam Teknologi Informasi dan Komunikasi. Jurnal Ilmiah Media Processor, 10(2).
- Gandrova, S., & Banke, R. (2023). Penerapan Hukum Positif Indonesia Terhadap Kasus Kejahatan Dunia Maya Deepfake. Madani: Jurnal Ilmiah Multidisiplin, 1(10).
- Gunawan, I. J., & Janisriwati, S. (2023). Legal Analysis on the Use of Deepfake Technology: Threats to Indonesian Banking Institutions. Law and Justice, 8(2). https://doi.org/10.23917/laj.v8i2.2513
- Irianto, S. (2017). Metode Penelitian Kualitatif Dalam Metodologi Penelitian Ilmu Hukum. Jurnal Hukum & Pembangunan, 32(2). https://doi.org/10.21143/jhp.vol32.no2.1339
- Laza, J. M., & Karo Karo, R. (2023). Perlindungan Hukum Terhadap Artificial Intellegence Dalam Aspek Penyalahgunaan Deepfake Technology Pada Perspektif UU PDP dan GDPR [Legal Protection of Artificial Intellegence in Misusage of Deepfake Technology in the Perspective of PDP Law and GDPR]. Lex Prospicit, 1(2). https://doi.org/10.19166/lp.v1i2.7386
- Leliana, I., Irhamdhika, G., Haikal, A., Septian, R., & Kusnadi, E. (2024). Etika Dalam Era Deepfake: Bagaimana Menjaga Integritas Komunikasi. Jurnal Visi Komunikasi, 22(02). https://doi.org/10.22441/visikom.v22i02.24229
- Marune, A. E. M. S. (2023). Metamorfosis Metode Penelitian Hukum. Civilia: Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan, 2(4).
- Muhammad Rifki Noval, S. (2019). Perlindungan Hukum Terhadap Korban Penyalahgunaan Data Pribadi: Penggunaan Teknik Deepfake. Seminar Nasional Hasil Penelitian & Pengabdian Kepada Masyarakat (SNP2M), November.
- Mutmainnah, A., Suhandi, A. M., & Herlambang, Y. T. (2024). Problematika Teknologi Deepfake sebagai Masa Depan Hoax yang Semakin Meningkat: Solusi Strategis Ditinjau dari Literasi Digital. UPGRADE: Jurnal Pendidikan Teknologi Informasi, 1(2). https://doi.org/10.30812/upgrade.v1i2.3702
- Novyanti, H. (2021). Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau Dari Hukum Pidana. Novum: Jurnal Hukum, 1(1).
- Rifa'i, I. J. (2023). Ruang Lingkup Metode Penelitian Hukum. Metodologi Penelitian Hukum.
- Saputra, A. (2018). Implementasi Kecerdasan Buatan Pada Proses Bisnis. Implementasi Kecerdasan Buatan Pada Proses Bisnis, 8(artifisial intelejen dalam bisnis).
- Sulaiman, S. (2018). Paradigma dalam Penelitian Hukum. Kanun Jurnal Ilmu Hukum, 20(2). https://doi.org/10.24815/kanun.v20i2.10076