Consumer Protection Strategies through Legal and Management Perspectives in the Era of Voice Cloning

Siti Risdatul Ummah
Universitas Safin Pati; Pati, Indonesia
E-Mail: siti_risdatul@usp.ac.id

Nur Wulan Intan Palupi
Universitas Safin Pati; Pati, Indonesia
E-Mail: nur_wulan@usp.ac.id

Submitted:
22 OCTOBER 2024

Accepted:
29 NOVEMBER 2024

ABSTRACT

The advancement of artificial intelligence technology, especially voice cloning, opens up opportunities for innovation while also presenting new risks in digital marketing. This study explores the potential for misuse of this technology to manipulate consumers through false promotions, using a legal and management perspective. Using a normative legal approach and literature study, this study analyzes regulations in Indonesia, such as the Information and Electronic Transactions Law, the Consumer Protection Law, and the Personal Data Protection Law, and compares them with practices in other countries. The results of the study indicate that regulations in Indonesia are not yet adequate to handle the complexity of voice cloning misuse, especially in consumer and personal data protection. Therefore, companies are advised to adopt strategies such as utilizing detection technology, increasing consumer digital literacy, and implementing stronger internal policies. This study highlights the importance of updating regulations that are more responsive to technological developments, including voice cloning. In addition, cross-sectoral collaboration between the government, industry players, and the community is key to protecting consumers while utilizing the potential of voice cloning technology responsibly and ethically.

***Keywords**: Consumer Protection, Managerial Strategy, Regulation, Voice Cloning*

ABSTRAK

Kemajuan teknologi kecerdasan buatan, khususnya voice cloning, membuka peluang inovasi sekaligus menghadirkan risiko baru dalam pemasaran digital. Penelitian ini mengeksplorasi potensi penyalahgunaan teknologi tersebut untuk manipulasi konsumen melalui promosi palsu, menggunakan perspektif hukum dan manajemen. Dengan pendekatan hukum normatif dan studi pustaka, penelitian ini menganalisis regulasi di Indonesia, seperti Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Konsumen, dan Undang-Undang Perlindungan Data Pribadi, serta membandingkannya dengan praktik di negara lain. Hasil penelitian menunjukkan bahwa regulasi di Indonesia belum memadai untuk menangani kompleksitas penyalahgunaan voice cloning, terutama dalam perlindungan konsumen dan data pribadi. Oleh karena itu, perusahaan disarankan mengadopsi strategi seperti pemanfaatan teknologi deteksi, peningkatan literasi digital konsumen, dan penerapan kebijakan internal yang lebih kuat. Penelitian ini menyoroti pentingnya pembaruan regulasi yang lebih responsif terhadap perkembangan teknologi, termasuk voice cloning. Selain itu, kolaborasi lintas sektoral antara pemerintah, pelaku industri, dan masyarakat menjadi kunci untuk melindungi konsumen sekaligus memanfaatkan potensi teknologi voice cloning secara bertanggung jawab dan beretika

***Kata kunci**: Perlindungan Konsumen, Strategi Manajerial, Regulasi, Voice Cloning*

JIAKES
Jurnal Ilmiah Akuntansi Kesatuan
Vol. 12 No. 6, 2024
pp. 467-476
IBI Kesatuan
ISSN 2337 – 7852
E-ISSN 2721 – 3048
DOI: 10.37641/jiakes.v12i6.3048

INTRODUCTION

The advancement of Artificial Intelligence (AI) technology continues to present innovations that change various aspects of life, including the way we communicate and do business (Rosidin et al., 2024). One technology that has stolen attention is voice cloning, which allows accurate duplication of a person's voice using AI-based algorithms. This technology brings great benefits, such as in the development of voice assistants, the entertainment industry, and customer service. However, like other technologies, voice cloning also has a dark side that raises concerns, especially in the context of misuse for promotional manipulation (Sakharina, 2013). In digital marketing, this technology is often misused to create the illusion of public figures, such as artists or celebrities, as if they are endorsing certain products or services, when in fact they have never been involved (Nasrullah, 2019). For example, in Indonesia recently, many advertisements circulating on social media platforms have shown videos of famous figures who are seen promoting illegal products, such as online gambling or slot games, which are clearly prohibited by the state.

Advertisements often feature voices that resemble public figures, when in fact, upon further investigation, the voices are produced through AI Voice Cloning without their knowledge or consent. This creates confusion and distrust among the public who feel they have been deceived (Koswara et al., 2024). This practice not only violates individual rights, such as the right to image and privacy, but also misleads consumers, who may believe that the promotion is legitimate and trustworthy. As a result, consumers are vulnerable to fraud that results in financial and psychological losses (Tamilselvan & Biswal, 2024). This threat has a wide impact, both from the perspective of consumers, companies, and society as a whole. For consumers, this fake promotion can lead to the purchase of products that do not meet expectations, and even potentially cause financial losses (Hakim & Budiarti, 2024). From a company perspective, this abuse can damage brand reputation and erode public trust. More broadly, this phenomenon shows the need for strategic steps involving legal and managerial approaches to protect consumers and ensure the ethical use of technology (Putra et al., 2024).

Through a legal approach, it is important to strengthen regulations related to the protection of individual rights, such as image rights and copyrights. Meanwhile, from a management perspective, companies can play a key role by educating consumers, increasing promotional transparency, and implementing policies that support business ethics (Pranata et al., 2023; Erislan et al., 2024). In an era where technology is increasingly complex, consumer protection is a top priority to ensure that technological innovation goes hand in hand with the values of integrity and trust (Widijowati, 2023; Aji et al., 2024; Irwansyah et al., 2024). Through this study, the author attempts to examine the threats and potential misuse of voice cloning from a legal and management perspective. This study is expected to provide strategic recommendations to protect consumers, both through stronger regulations and more proactive managerial steps.

METHODS

This study employs a normative legal approach, utilizing library research that relies on secondary data (Sunggono, 2018). The methodology aligns with the legal problem's substance, employing a statutory and analytical descriptive approach. The statutory approach examines applicable regulations, while the analytical descriptive approach delves into the legal framework and its practical implications. Focusing on the crime of voice cloning, the study identifies, analyzes, and interprets legal standards from various sources. Primary data includes laws and regulations such as the Information and Electronic Transactions (*Informasi dan Transaksi Elektronik*/ITE) Law (Law No. 19 of 2016), Law No. 27 of 2022 on Personal Data Protection, and articles in the Criminal Code, specifically Article 378 on fraud and Articles 310–311 on defamation or slander.

Secondary data comprises legal literature, expert opinions, articles, journals, theses, books, and other relevant scientific works. This secondary data enriches the understanding and analysis of voice cloning as a legal issue.

RESULTS AND DISCUSSION

Misuse of Voice Cloning Technology: Threats and Regulatory Implications

Advances in artificial intelligence technology have enabled the creation of voice cloning technology, which is the ability to replicate the human voice with a very high level of accuracy. Although this technology offers significant benefits in various sectors, such as the development of virtual assistants, the entertainment industry, and customer service, the risk of its misuse cannot be ignored. Misuse of voice cloning technology has become a real threat, especially in cases of fraud, identity theft, and privacy violations. One of the most common forms of misuse is voice-based fraud. In this case, voice cloning technology is used to imitate the voice of a particular individual, usually a public figure, authority figure, or family member, in order to manipulate the victim into handing over personal information or funds. This mode is increasingly difficult for the public to recognize, given the level of precision of the technology that is able to produce a voice replica that is very similar to the original.

In addition, voice cloning has also been used to steal someone's identity, which is then used in illegal activities, such as accessing financial accounts, deceiving institutions, or even damaging an individual's reputation. In a broader context, privacy violations are also an important issue, especially when a person's voice is replicated without their knowledge or consent. This is not only detrimental to the individual but also raises ethical challenges in the use of technology. In the public sector, the misuse of this technology can threaten the stability and public trust in institutions. For example, the use of voice cloning to spread false information (hoaxes) or misleading messages that appear to come from government officials can trigger social unrest. In the business world, this misuse can also be detrimental to companies, especially if the voices of executives or staff are used to give false instructions to employees or business partners.

One case of misuse of voice cloning involving a public figure to deceive consumers occurred when the voice of a famous celebrity was replicated to promote a fake investment product. In this case, the fraudster used voice cloning technology to create an audio recording that resembled the celebrity's voice, claiming that he personally endorsed and used a particular investment service. The recording was distributed through digital advertisements and social media platforms, convincing many consumers that the product was legitimate. Many victims ended up handing over their money to an investment platform that turned out to be a scam. After this case was exposed, the celebrity clarified that he was never involved in the promotion and was a victim of manipulation by voice cloning technology. This case highlights the dangers of misusing this technology to create false trust, deceive consumers, and harm the reputation of the targeted public figure.

The biggest challenge in dealing with voice cloning abuse is the lack of regulations that specifically regulate this technology. Most of the current legal frameworks are inadequate to deal with the complexity of the problems caused by voice cloning technology. In addition, public awareness of the risks posed by this technology is still relatively low, increasing the vulnerability to abuse. Therefore, strategic steps are needed that involve various parties, including the government, technology providers, and the community. Strong regulations must include aspects of security, protection of individual rights, and law enforcement against violations. On the other hand, public education and global collaboration need to be increased to ensure that this technology is used responsibly. Misuse of voice cloning technology is not only a technological issue, but also a social, legal, and ethical challenge. Therefore, a holistic approach is needed to minimize its impact while utilizing this technology positively for the common good.

Consumer Protection from Voice Cloning Crimes: Legal Perspective in Indonesia

The development of information technology today tends to make society experience major changes, technological progress and development can have an impact on human culture in both positive and negative ways (Rizky, 2024). The increasing use of information and communication technology, especially on social media, will also affect the increase in various types of cyber-based crimes. One example of cybercrime is the crime of developing artificial voice technology called Voice Engine. is one of the new types of crimes in the modern world that is based on technological sophistication and has a universal nature in the scope of cyberspace, so that it can have a negative impact on consumers that are not felt physically but are just as detrimental as other crimes (Novita & Santoso, 2021).

Misuse of voice cloning technology can have an impact on consumers, especially in the form of fraud, namely the perpetrator uses an imitation voice to ask for money or personal information from consumers, identity theft can be done by imitating the voice to access services in the name of the victim, such as banking or digital platforms, or violations of privacy, namely the use of consumer voices without permission violates the right to personal data. To protect consumers, a clear and effective legal framework is needed. Law is a rule about how individuals should act as members of society in order to maintain order, safety and happiness. As a country of law, Indonesia has established laws related to criminal acts of fraud and protection of personal data both in the Criminal Code (*Kitab Undang-Undang Hukum Pidana*/KUHP) and in special laws. However, in relation to the crime of Voice Cloning itself, there is no special law that regulates it, but by using the elements that generally exist, legal protection for consumers can be established using the ITE Law, Basic Agrarian Law (*Undang-Undang Pokok Agraria*/UUPK), Personal Data Protection (*Perlindungan Data Pribadi*/PDP) Law and the Criminal Code.

Legal policies related to consumer protection in Law No. 19 of 2016 concerning ITE in Article 28 paragraph (1) which states that Every Person intentionally and without the right to spread false and misleading news that results in consumer losses in Electronic Transactions. This article aims to protect the public, especially consumers from the negative impacts of the spread of false (hoax) or misleading information related to electronic transactions. Electronic transactions cover various commercial activities carried out via the internet, such as purchasing goods/services, banking, or online investment, in addition, this article also encourages the responsibility of service providers, business actors, and individuals in disseminating valid and accurate information. Violations of Article 28 paragraph (1) can be subject to penalties in accordance with the criminal provisions contained in the ITE Law. The criminal threat can be in the form of a maximum imprisonment of 6 years, and/or a maximum fine of IDR 1 billion, while Article 29 regulates the prohibition of the use of information technology to send threats or intimidation carried out via electronic media, be it text messages, email, social media, or other platforms. Violations of Article 29 of the ITE Law are subject to criminal sanctions in accordance with Article 45B of the ITE Law, a maximum imprisonment of 4 years, and/or a maximum fine of IDR 750 million.

Consumer Protection from Voice Cloning Crimes is also regulated in Law No. 8 of 1999 concerning Consumer Protection UUPK in Article 4 it is explained that Consumers have the right to security, comfort and safety in using goods/services, including protection from technology-based fraud, Consumers also have the right to obtain legal assistance or dispute resolution if there is a problem with the business actor, in addition if there is a loss caused by goods or services that are not in accordance, the consumer has the right to a reasonable replacement. Sanctions related to violations of consumer rights as regulated in Article 4 of Law No. 8 of 1999 concerning Consumer Protection are explained in other parts of the law, especially Chapter XI (Criminal Provisions) and Chapter X (Compensation Provisions). Criminal sanctions in Chapter XI - Article 62 of the UUPK explain that if a business actor violates consumer rights, including intentionally providing false information, goods and services that are not in

accordance, or harm consumers, they can be subject to a maximum imprisonment of 5 years or a maximum fine of IDR 2 billion, this provision includes violations that endanger consumers or are carried out in bad faith, such as selling unsafe products, providing misleading information, or not fulfilling compensation obligations. The sanctions for Compensation Obligations are contained in Chapter X - Article 19 of the UUPK explaining that if consumers are harmed by goods or services that do not comply with the initial agreement or can cause losses, then the perpetrator who has a business is required to provide a refund according to the value of the product/service, Replacement of goods/services with appropriate or equivalent, Compensation for additional losses, including physical damage, health, or even death due to the goods/services provided. The compensation must be given within a maximum of 7 days after the decision or official request from the consumer.

Personal Data Protection is included in the category of human rights protection. Therefore, regulations related to Personal Data are a manifestation of recognition and protection of basic human rights. The existence of the Law on Personal Data Protection is a must because this Law can protect various national interests. This protection can also facilitate transnational trade, industry, and investment transactions. The Law on Personal Data Protection is a mandate from Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia which states that, "Everyone has the right to protection of personal data, family, honor, dignity, and property under his control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a basic human right." The issue of Personal Data Protection arises due to concerns about violations of Personal Data that can be experienced by individuals and/or legal entities. Such violations can result in material and non-material losses.

Law No. 27 of 2022 concerning PDP Article 3 explains that Personal data, including voice, is protected by law. The use of voice without permission can be considered a violation of privacy. Sanctions for Violation of the provisions of the PDP Law can be subject to Administrative sanctions, namely Reprimands, administrative fines, temporary suspension of activities, to deletion of data, while Criminal sanctions are Fines and/or imprisonment for individuals who are proven to have intentionally misused personal data. Article 378 of the KUHP can also be used to protect consumers who are victims of Voice Cloning, Article 378 of the Criminal Code reads, "Anyone who with the intention of benefiting themselves or others unlawfully, by using a false name, false dignity, trickery, or a series of lies, moves another person to hand over an object, give debt, or write off receivables, is threatened with fraud with a maximum imprisonment of four years."

According to Sugandhi (1980), the elements of the crime of fraud contained in Article 378 of the Criminal Code are the actions of a person with trickery, a series of lies, a false name and a false state with the intention of benefiting themselves without rights. Meanwhile, according to Soesilo (1995), the crime in Article 378 of the Criminal Code is called *fraud*, where the fraudster is his job. Fraud using technology such as voice cloning can be categorized as a crime of fraud, Perpetrators who are proven to have committed a crime of fraud based on Article 378 of the Criminal Code can be subject to a maximum imprisonment of 4 years. If consumers become victims of voice cloning abuse, they can file a report with the police or relevant authorities by bringing evidence of fraud or violations, consumers can also file a lawsuit for damages based on the UUPK or the PDP Law, in addition consumers can ask for help from institutions such as National Consumer Protection Agency (*Badan Perlindungan Konsumen Nasional*/ BPKN).

Evaluation of Regulations in Indonesia with Other Countries

The development of technology, especially AI, has brought significant changes in various aspects of life, including in the realm of privacy and personal data security. Artificial intelligence enables large-scale and high-speed data analysis, which has an impact on increasing the potential for data misuse that ultimately threatens individuals'

digital civil rights (Novita & Santoso, 2021). In Indonesia, regulations related to criminal acts of voice cloning have been regulated through various laws, such as the ITE Law (Law No. 19 of 2016 concerning Information and Electronic Transactions), the Personal Data Protection Law and the Criminal Code. However, the biggest challenge today is how to ensure that these regulations are able to keep up with the pace of technological development, especially in the context of artificial intelligence, which has its own dynamics and risks. At the global and national levels, governments are working hard to control the unethical use of AI voice technology. For example, the United States through the Federal Communications Commission has taken proactive action by banning the use of robocalls that use AI voices to imitate public figures. This step is a response to concerns about the increase in annoying spam calls. However, the situation in Indonesia provides a deeper picture of the potential negative impacts of misuse of voice cloning technology. According to the Ministry of Communication and Information, there were 1,730 cases of online fraud with losses reaching hundreds of trillions of rupiah until November 2022. Furthermore, the National Police have handled 39,586 cases of fraud and embezzlement during the same period, highlighting the scale of this problem.

The potential risks of misuse of voice cloning technology are very real in Indonesia. The Ministry of Communication and Information reported that the number of victims of online fraud reached 130,000 people in 2022, with increasingly sophisticated methods, including the use of fake identities through voice cloning technology. The development of artificial voice technology by OpenAI through Voice Engine opens up great opportunities for positive use in various sectors, but also carries significant risks, especially related to online security. In Indonesia, cases of online fraud and embezzlement involving voice cloning technology are a serious concern for the government and the public. The importance of improving digital literacy and online security cannot be ignored. The government needs to work with related institutions and technology companies to develop adequate regulations and prioritize privacy and security aspects in the development of AI voice cloning technology. With the right steps, the positive potential of this technology can be utilized optimally without sacrificing public security and privacy (Prayuti, 2024).

Recommendations for Regulatory Updates to Protect Consumers from Voice Cloning Abuse

Voice cloning technology that uses artificial intelligence to imitate the human voice has presented great opportunities in various sectors, such as entertainment, education, and customer service. However, this progress has also raised concerns about the potential for misuse, including in cases of fraud, identity theft, and privacy violations. To address these challenges, comprehensive regulatory reforms are needed to protect consumers from the negative impacts of this technology (Alviani, 2024). First, regulations need to improve the security standards of voice cloning technology by ensuring that the software can only be used by authorized parties. One important step is the implementation of an identity verification mechanism that can ensure that only legitimate voice owners have access to replicate their voices. In addition, voice cloning software must go through a certification process carried out by a supervisory agency to ensure its compliance with established security standards.

Second, regulations must also provide protection for the rights and consent of voice owners. A person's voice should be considered part of their intellectual property rights, which means that any use of this technology must have the explicit consent of the voice owner. This consent must be formally documented and auditable to avoid violations. In addition, voice owners need to have exclusive rights to control how their voices are used, as well as the ability to sue for violations of those rights. Transparency is also an important element in regulation. Any use of voice cloning in public interactions must be clearly communicated to the parties involved. Digital content that uses synthetic voices must be explicitly labeled to avoid potential misinformation. This step aims to ensure

that consumers can distinguish between real voices and voice cloning technology. Law enforcement against the misuse of this technology must also be prioritized. Misuse of voice cloning for purposes such as fraud, identity fraud, or violation of privacy must be categorized as a criminal offense that can be subject to strict sanctions. In addition, regulations need to provide a complaint mechanism that allows the public to report cases of misuse of this technology easily and quickly (Novita & Santoso, 2021).

To support the effectiveness of regulation, increasing digital literacy in the community is essential. Public education programs should focus on increasing understanding of voice cloning technology, the risks involved, and how to protect themselves from misuse. Law enforcement officers must also receive special training to be able to handle cases related to this technology effectively. Finally, regulatory reforms need to take into account the global dimension, given the cross-border nature of digital technology. Collaboration with other countries and the adoption of international standards are important steps to ensure broader consumer protection. In addition, the establishment of a special supervisory body that focuses on supervising artificial intelligence technology, including voice cloning, can provide a long-term solution to prevent misuse. With comprehensive regulatory reforms, the risk of misuse of voice cloning technology can be minimized, so that this technology can be used safely and responsibly for the benefit of society.

Managerial Strategies to Protect Consumers

Voice cloning has the ability to accurately replicate the human voice. This technology also has the potential to be misused for fraud, such as identity theft or consumer manipulation. In addition to regulatory updates, companies must also design managerial strategies to protect consumers from this threat. The use of Voice Cloning in advertising includes the potential for misuse of technology for fraud and manipulation, which can have a negative impact on brand reputation and consumer trust (Koswara et al., 2024). Managerial strategies to address this threat must include three main pillars, namely the use of technology for detection, increasing consumer digital literacy, and strong internal company policies.

Utilizing Technology to Detect Voice Cloning

Technology is a fundamental element in detecting and preventing voice cloning abuse. The use of a voice biometric system can distinguish the original voice from the duplicated voice. This system works by analyzing a person's unique voice patterns, such as pitch frequency or intonation (Thiraviyam, 2018). This technology not only increases the security of voice-based transactions but also prevents potential fraud. For example, bank customer service can utilize voice biometrics to verify customer identity more securely. AI-based monitoring systems can be used to monitor suspicious digital communication patterns. With sophisticated algorithms, the system can provide automatic alerts if a voice that is not original is found (Sruthi & Shanjai., 2021). Companies can partner with digital security technology providers to develop increasingly sophisticated detection tools. Investment in this innovation, although expensive, can reduce significant risks to consumers and the company's reputation (Suarmanayasa et al., 2024; Rany et al., 2024).

Consumer Education Through Digital Literacyl

In addition to technology, adequate digital literacy allows consumers to recognize the risks of voice cloning and protect themselves. Companies can launch educational campaigns explaining what voice cloning is, how the technology works, and the risks it poses (Muhtadi & Sahrul, 2023). These campaigns can be disseminated through social media, company websites, and other communication platforms. Simple guidelines, such as never give personal information over the phone without verification or Use additional passcodes in important communications, can help consumers avoid falling into voice-based fraud traps. In addition to campaigns, interactive training programs can be

designed for consumers, especially those who frequently use voice-based technology. This training can include simulations of fraudulent situations and how to identify threats.

Internal Company Policies to Prevent Technology Abuse

Internal company policies play an important role in preventing misuse of voice cloning technology by both internal and external parties. Companies must have written policies that govern the use of AI technology, including voice cloning. Periodic internal technology audits can ensure that AI systems operate in accordance with established policies (Priowirjanto, 2022). This oversight can also identify potential security gaps that need to be addressed immediately. Companies must train employees to understand voice cloning technology, the risks involved, and their responsibilities in protecting consumers. This training not only improves employee competence but also builds a corporate culture that is oriented towards consumer protection.

Collaboration Between Stakeholders

Managerial strategies cannot stand alone without support from regulators, technology providers, and consumers. Therefore, companies need to actively participate in discussions and the formation of regulations relevant to consumer protection. And collaborate with other companies to share best practices and build common security standards. Invite input from consumers about their experiences with the company's technology to continuously improve protection policies.

CONCLUSION

The misuse of voice cloning technology in digital marketing poses significant threats to consumers, including fraud, privacy violations, and identity theft. In Indonesia, existing regulations address some aspects of this issue but lack specificity to tackle its growing complexity. Comprehensive regulatory updates are essential, such as recognizing voice as intellectual property, mandating labelling of synthetic voices, and enforcing strict penalties for misuse. Beyond regulations, managerial strategies are crucial for consumer protection. Companies should adopt advanced detection technology to identify synthetic voices and implement internal policies focused on ethical practices. Public education campaigns are also vital to raise awareness of potential risks and promote safe interactions with voice-based technologies. Global collaboration and enhanced digital literacy can further ensure responsible use of voice cloning technology. Stakeholders, including governments, companies, and civil society, must work together to create ethical frameworks and share best practices. By combining robust regulations, proactive management, and community engagement, voice cloning can be harnessed ethically, benefiting society while minimizing risks to consumers.

REFERENCES

[1] Aji, B. A., Ikhlas, D. I., & Wati, I. R. (2024). Human resource competency development in facing the challenges and opportunities of the industry 4.0 era. *Research Horizon*, *4*(6), 301-308.

[2] Alviani, A. (2024). Legal regulations on criminal acts against misuse of ai (artificial intelligence) technology in voice phishing fraud via mobile phones. *Jurnal Hukum De'rechtsstaat*, *10*(2), 207-216.

[3] Erislan, E. (2024). Analysis of marketing management strategies in facing dynamic consumer behavior in the digital era. *Jurnal Ilmiah Manajemen Kesatuan*, *12*(2), 365-372.

[4] Hakim, M. M., & Budiarti, W. (2024). How false advertising victims' experiences define their online purchase decision in fashion product?-comparison between generations. *JDM (Jurnal Dinamika Manajemen)*, *15*(2), 250-268.

[5] Irwansyah, I., Sari, R. R., Hasanuddin, H., & Rumianti, S. (2024). Protection of consumer privacy in the use of big data in the digital economy. *Jurnal Ilmiah Manajemen Kesatuan*, *12*(3), 561-564.

[6] Koswara, A. (2024). Eksploitasi ai voice cloning dalam pemasaran digital: analisis kebohongan dan manipulasi suara dalam iklan. *Jurnal Imagine*, *4*(2), 77-83.

[7] Muhtadi, M. A., & Sahrul, S. (2023). Hukum perlindungan konsumen dan etika bisnis di era teknologi kecerdasan buatan: perlindungan pengguna dan tanggung jawab perusahaan. *Jurnal Hukum dan HAM Wara Sains*, *2*(09), 922-930.

[8] Nasrullah, D. (2019). *Teori etika*: *Keperawatan keluarga*. Surabaya: Universitas Muhammadiyah Surabaya.

[9] Novita, Y. D., & Santoso, B. (2021). Urgensi pembaharuan regulasi perlindungan konsumen di era bisnis digital. *Jurnal Pembangunan Hukum Indonesia*, *3*(1), 46-58.

[10] Pranata, W., Valevi, S., Habibullah, M., Sari, R., & Nofirda, F. (2023). Social media as a tool in improving public relations in the digital marketing era: qualitative insights. *Jurnal Ilmiah Manajemen Kesatuan*, *11*(3), 1211-1220.

[11] Prayuti, Y. (2024). Dinamika perlindungan hukum konsumen di era digital: Analisis hukum terhadap praktik e-commerce dan perlindungan data konsumen di Indonesia. *Jurnal Interpretasi Hukum*, *5*(1), 903-913.

[12] Priowirjanto, E. S. (2022). Urgensi pengaturan mengenai artificial intelligence pada sektor bisnis daring dalam masa pandemi covid-19 di indonesia. *Jurnal Bina Mulia Hukum*, *6*(2), 254-272.

[13] Putra, P., Asike, A., Syahril, M. A. F., & Andirwan, A. (2024). Sinergi manajemen pemasaran, sdm, dan kepatuhan hukum ITE: strategi terpadu dalam pengelolaan perguruan tinggi di era digital. *Jurnal Ilmiah Manajemen & Kewirausahaan*, *10*(3), 189-194.

[14] Rany, Y., Indradewa, R., Abadi, F., & Kustiawan, U. (2024). Strategic financial planning analysis to deliver sustainable profits. *Jurnal Ilmiah Manajemen Kesatuan*, *12*(6), 2609-2618.

[15] Rizky, A. A. M. (2024). Legalitas alat bukti rekaman suara dalam tindak pidana cyber ditinjau dari UU ITE. *Jurnal Rechtswetenschap: Jurnal Mahasiswa Hukum*, *1*(1).

[16] Rosidin, R., Novianti, R., Ningsih, K. P., Haryadi, D., Chrisnawati, G., & Anripa, N. (2024). Peran kecerdasan buatan dalam pengembangan sistem otomatisasi proses bisnis. *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, *7*(3), 9320-9329.

[17] Sakharina, I. K. (2013). Pengungsi dan HAM. *Jurnal Hukum Internasional*, *1*(2), 198-221.

[18] Soesilo, R. (1995). *Kitab undang-undang hukum pidana (kuhp): serta komentar-komentarnya lengkap pasal demi pasal*. Bogor: Politeia.

[19] Sruthi, M. S., & Shanjai, K. (2021, May). Automatic voting system using convolutional neural network. In *Journal of Physics: Conference Series* (Vol. 1916, No. 1, p. 012074). IOP Publishing.

[20] Suarmanayasa, I. N., Pramesworo, I. S., Masela, A., Sucipto, B., & Launtu, A. (2024). Risk management strategies in the financial industry theoretical review and practical implications. *Jurnal Ilmiah Manajemen Kesatuan*, *12*(4), 995-1004.

[21] Sugandhi, R. (1980). *Kitab undang-undang hukum pidana*. Surabaya: Usaha Nasional.

[22] Sunggono, B. (2003). *Metodologi penelitian hukum*. Yogyakarta: Raja Grafindo Persada.

[23] Tamilselvan, G., & Biswal, M. (2024). Voice cloning & deep fake audio detection using deep learning. *International Journal of Advanced Research and Interdisciplinary Scientific Endeavours*, *1*(2), 22-26.

[24] Thiraviyam, T. (2018). Artificial intelligence marketing. *International Journal of Recent Research Aspects, 19* (4), 449-452.

[25] Widijowati, D. (2023). Enhancing consumer protection in electronic commerce transactions. *Research Horizon*, *3*(4), 283-290.