Vol. 2, No. 1, pp. 41-47 | 2024
CFORSJ Procedia

A REVIEW OF EMERGING CRIMES AND CHALLENGES ARTIFICIAL INTELLIGENCE (AI) MANIPULATION IN DIGITAL ADVERTISING FROM A MALAYSIAN LEGAL PERSPECTIVE

[i]Tuan Muhammad Faris Hamzi Tuan Ibrahim, [i]Muhammad Sobri Faisal, [ii,iii,iv,v,]*Ahmad Syukran Bin Baharudin & [ii,iii]Mohamad Aniq Aiman Alias

[i]Faculty of Social Sciences and Humanities, Universiti Teknologi Malaysia (UTM), 81310, Skudai, Johor, Malaysia
[ii]Faculty of Syariah and Law, Universiti Sains Islam Malaysia (USIM), 71800, Nilai, Negeri Sembilan, Malaysia
[iii]Centre of Research for Fiqh Forensics and Judiciary (CFORSJ), Faculty of Syariah and Law, Universiti Sains Islam Malaysia (USIM), 71800, Nilai, Negeri Sembilan, Malaysia
[iv]International Advisory Board Member, Mejellat Al-Afaq wa Al-Maarif (JSKP), Faculty of Humanities, Islamic Sciences and Civilization, University Amar Telidji of Laghouat, BP 37G, Road of Ghardaia, 03000 Laghouat, Algeria
[v]Associate Editor, Journal of Contemporary Maqasid Studies, Maqasid Institute, United States of America (USA)

*(Corresponding author) e-mail: ahmadsyukran@usim.edu.my

ABSTRACT

Artificial Intelligence (AI) has spread quickly throughout Malaysia's business, education, healthcare, and security sectors. AI provides strong tools for evaluating customer data, improving user experiences, and refining targeted advertisements in digital advertising. But there are some drawbacks to this quick expansion as well, most notably the abuse of AI in cybercrimes. These days, technologies like DeepFake make it possible to produce incredibly lifelike yet fake content, which raises moral and legal questions. Since Malaysia does not yet have particular laws to handle the complexity of crimes involving artificial intelligence, it is difficult for law enforcement to find and bring charges against criminals. This study aims to investigate the effects of artificial intelligence (AI) manipulation in digital advertising, evaluate the efficacy of Malaysia's current legal system, and suggest ways to overcome its limitations. In order to tackle these problems effectively and ensure safeguards, against AI misuse in the realm of advertising in Malaysia this study uses document analysis to pinpoint key gaps in the current legal framework. The research underscores the necessity for guidelines to govern AI altered content as the absence of a legal structure hinders effective regulation. As a solution, the study proposes the establishment of a framework for AI alongside measures such as improving law enforcement training and investing in cutting edge technological infrastructure. It's crucial to follow these suggestions to uphold secure advertising practices while safeguarding individuals and businesses from potential risks associated with AI driven offenses.

Keywords: *Artificial Intelligence (AI), cybercrime, digital advertising, civil court*

Introduction

Artificial intelligence represents the most propelling technology of the present times and will, therefore, unleash an impact upon governments, businesses, and economies all around the world including that based in Malaysia (Dubey, 2024). This brings about a wider scope of capabilities on areas from the manufacturing and banking to healthcare and education sectors in terms of increasing efficiencies of functions as well as extending simulation of human executive intelligence that assists with decision-making. Some of them are data analysis, natural language understanding, and automation that contribute toward creativity and offer insights that are beyond error. Such characteristics make this an approach that any individual or corporation would fancy (Shrivastava, 2024).

AI has been redefining patient care in the health sector. It provides improved speed and accuracy of diagnosis through a vast array of medical data-aiding pattern identification-and suggested possibilities in terms of conditions or treatment, with a level of precision that compliments human expertise (Dubey, 2024). In doing predictive analytics, AI systems can warn healthcare providers about patient needs, thereby allowing for more efficient resource management and, ultimately, improved outcomes for patients. For education, according to Faraasyatul 'Alam et al., (2024), AI has also transformed traditional learning methods. Adaptive learning systems can adjust the content of education to a student's progress and his strengths and weaknesses, thus creating an adjoined learning experience. AI-driven tools, such as virtual tutors and intelligent assessment systems, may be used to create a more engaging and supportive learning environment that makes education more accessible to each student in line with their peculiar needs. In security, H Patel and Gera (2024) state that uses of AI range from facial recognition and biometric systems to predictive policing and intelligent surveillance. AI provides direct monitoring systems where it analyses footage from TV cameras or other sensor arrangements in real-time, detects unusual activity, and alerts the authorities about possible threats, hence improving public safety. They even protect national security, giving aid to governmental agencies in the observation and supervision of complex problems presented in the cyber world.

However, alongside those transformations triggered by AI, comes also a lot of concerns typically raised within the spheres of cybersecurity and law enforcement. The features used in AI for improving sectors like healthcare or education can also be misused by criminals. AI is used by criminals for identity thefts, digital fraud, and other nefarious activities (Mathew, 2024). Such AI-generated fakes mimic real humans' expressions and voices so closely that they can be nearly impossible to detect with a naked eye. However, this poses massive risks for personal data behind closed doors, from the reputation of corporations to the extremely delicate ball of public trust.

The legal framework in Malaysia and in other countries face an urgent need to adapt to new AI-driven threats. The conventional laws have for long lacked enough tools for controlling crimes with the pace of developing technology. Every time a new AI evolves in a new or sophisticated way, the regulations still provide unambiguous consequence of intent or accountability, thus posing problems to the prosecution. It requires collaboration between the lawyers, technologists, policymakers, and people from industry to create a robust framework of regulations, which could provide for AI's benefits with strict oversight. Concerning the future, Malaysia is at the pivotal joining point of, on one end, accepting AI, and on the other, protecting itself from its dangers. In preparing for the future where AI technology prevails, it would take shipment of reinforcement on mechanisms of enforcement and instituting pro-active policy intervention so as to steer Malaysia towards responsible use of AI amid its safe sustainability. This journey requires reaffirmation of expertise in technology that goes hand in hand with building legal capabilities. But this sets into motion an awareness and vigilance promotion towards the triggered possibilities of risks and ethics that would meet with public awareness, allowing that citizens would act together employing AI technologies for social good while minimizing adverse effects.

Methodology

In order to respond to the issues posed by the misuse of AI, this study uses document analyses to impose a very critical lens on existing legal frameworks and discern major gaps. Document analysis is referred to as reviewing and interpreting legislative documents, statute reports, and relative texts of laws with the intention of deciphering the prevailing themes, inconsistencies, or shortcomings present in current laws governing AI technologies.

The research aims at establishing areas in which current legislation appears unclear or lacks applicable enforcement mechanisms with respect to crimes committed under the futuristic guise of AI. This involves the very scrutiny of policies, regulative codes, judicial-like interpretations, and the various infringement guidelines as they relate to the better use or improper misuse of AI. This analysis is also going to be both qualitative and interpretive, centering on the legal texts to provide an understanding of the stated strengths and weaknesses of the model in force while establishing precisely where some reforms or further guiding instructions for the process may be necessary.

Result and Discussion

Manipulation AI In Digital Advertising

The integration of artificial intelligence into digital advertising has reshaped the industry into new opportunities with unprecedented challenges. On the rise of ad revenues, digital platforms including Facebook, Instagram, TikTok, and X are on exponential growth partly due to the increase in online engagement during the COVID-19 pandemic (Chauhan & Thakur, 2023). With the rise of brands and advertisers trying to catch consumers' attention, AI has become an important constituent in creating focused individualized ad campaigns. From analyzing user behavior to optimization of ad placements, the algorithms of AI allow companies to reach specific demographics with tailored content that resonates more deeply with users.

However, the rapid of AI technology has introduced severe security risks and ethical concerns. A prominent example is DeepFake technology which allows for the creation of highly realistic AI generated videos (Amerini et al., 2024). Initially developed for entertainment applications such as face-swapping, DeepFake technology has quickly evolved to include more complex manipulations, like lip-syncing, which can convincingly depict individuals saying things they never actually said. While these applications are often harmless in entertainment, their misuse has raised alarm bells due to the potential for widespread deception and fraud.

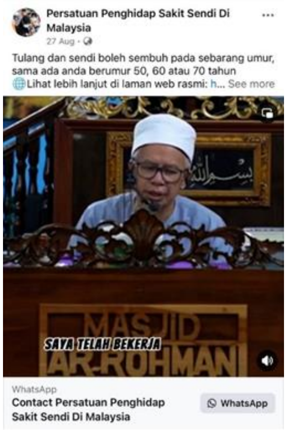
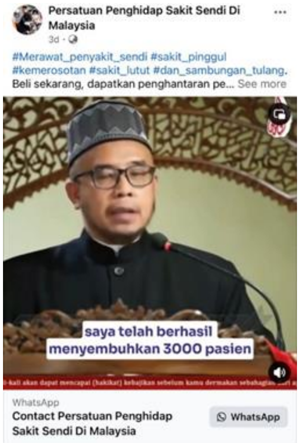
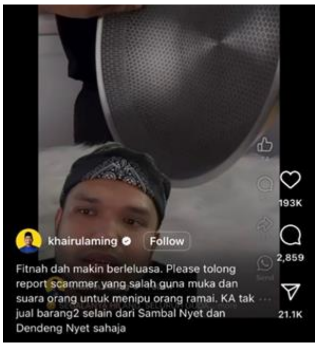
DeepFake technology is dangerously used in various fields of digital advertising for manipulation and unauthorized use specifically regarding public figures. Using video generated by AI, designers can show celebrities promoting a product or service that they did not approve of. For instance, you could be witnessing a DeepFake of a well-known face endorsing a particular brand, which may give an illusion to the people that the endorsement is real. Such exploitation not only impacts the rights of individuals featured in these synthetic videos, but also undermines public trust in digital content and online advertising as a whole.

There are serious ethical and legal implications for advertising fast with DeepFake. Rendering public figures, including (but not limited to) ordinary people as mere objects of brand-image conveyance without their consent is an infringement on personal right that not only has the potential to inflict reputational harm but psychological trauma when considered in extreme cases. Also, consumers misled by deceptive AI-created content may unwittingly endorse brands or products under false pretenses a scenario with potentially grave financial and social ramifications.

The potential problem is that the AI technologies are slowly getting more sophisticated and tougher to recognize. There are some AI-generated contents, which is impossible to differentiate them between a real media and some other features of digital media, as well same feature is there that we may not be able to do verify or check their authenticity by viewers or even system. Consequently, this will put the burden on digital platforms and regulators to maintain tight coiled discretion from spreading fraudulent DeepFake Ads. Advanced detection algorithms, watermarking of genuine content, and mandatory disclosure of AI-generated media are some countermeasures against these types of risks.

Here, an AI manipulation case in digital advertising can be defined with some real-life world examples that display both sides of the potential as well as risk side. Such instances show how AI can be misused for misinformation, compromise public persons and manipulate consumers therefore there must be robust safeguards.

Table 1. Show three examples of AI manipulation cases

Example of AI Manupulation Cases	
 Persatuan Penghidap Sakit Sendi Di Malaysia 27 Aug · Tulang dan sendi boleh sembuh pada sebarang umur, sama ada anda berumur 50, 60 atau 70 tahun 🌐Lihat lebih lanjut di laman web rasmi: h... See more SAYA TELAH BEKERJA WhatsApp Contact Persatuan Penghidap Sakit Sendi Di Malaysia 	This video demonstrates AI manipulation in digital advertising. The message is a video of a reputable former religious minister endorsing a health cure for joint ailments, shared by an organisation on social media. The video title suggests that the individual supports or has collaborated with the organisation, which may not be accurate. This manipulation, likely facilitated by deepfake technology, seeks to use the trust and influence of significant community actors to enhance the product's legitimacy.
 Persatuan Penghidap Sakit Sendi Di Malaysia 3d · #Merawat_penyakit_sendi #sakit_pinggul #kemerosotan #sakit_lutut #dan_sambungan_tulang. Beli sekarang, dapatkan penghantaran pe... See more saya telah berhasil menyembuhkan 3000 pasien WhatsApp Contact Persatuan Penghidap Sakit Sendi Di Malaysia 	One of the posts, also referred to as "joint pain," features a video with Mufti Perlis, who claims that this medicine is endorsed by someone and has the potential to cure numerous gastrointestinal ailments. Nevertheless, the person in the video may not have genuinely endorsed this product; it might merely be an artificially made video or an edited version that mimics authentic endorsement.
 khairulaming Fitnah dah makin berleluasa. Please tolong report scammer yang salah guna muka dan suara orang untuk menipu orang ramai. KA tak jual barang2 selain dari Sambal Nyet dan Dendeng Nyet sahaja 	This graphic exemplifies AI manipulation, as popular figure Khairul Aming cautions his fans of scammers exploiting his likeness and voice to endorse things he does not support. In this instance, AI technologies such as deepfake and speech synthesis also have been employed to generate persuasive content.

Emerging Crimes from AI Manipulation

With the potential misuse of AI technology now more entrenched and bigger, new crimes in relation to manipulation of AI provide some unique challenges for existing legal frameworks. In particular, those acts and provisions in Malaysia which relate to new crimes of this nature mainly involve deception-based activities, impersonation or unauthorized endorsement, intrusion into individual's privacy by way of image/video capturing or recording using modern technology as well as platform (s) for the distribution or dissemination of defamatory content (s). The following is a list of the legal instruments available that could be used to regulate and penalize AI-related crimes:

First and foremost, Communications and Multimedia Act 1998 (Act 588). Among the principal legislation governing online and digital activities in Malaysia is the Communications and Multimedia Act 1998 (Act 588). There are portions of the Act that specifically regulate offensive and improper content. The said act prohibits content that may cause harm or mislead, while creation, distribution, and hosting are under Section 211 on offensive contents. This provision can be used to hold responsible individuals or entities distributing misleading content for any reputational harm caused by the distribution of AI-manipulated media, such as deepfakes or non-consensual "deepfake" endorsements. In addition, Section 233 will deal with the misuse of network facilities service These can include instances in which deployment of an AI system facilitates the dissemination of false content over any digital platform. Therefore, making these sections crucial in governing digital ad practices and keeping the individual out from becoming a digital victim.

Other legislation may also come into play such as the Personal Data Protection Act 2010 (Act 709), which concerned itself with protecting personal data from unlawful use. Such AI manipulations typically involve the non-consensual use of individual's likenesses, voices or other identifiable characteristics, which is a clear breach of privacy. An example of a violation for this act is creating a deepfake leveraging the image or voice of another not authorized to do so, which constitutes an unauthorized use or misappropriation of personal data. This is specifically applicable to identity theft, fraud, or unauthorized endorsements done through the use of all AI technologies.

The Copyright Act 1987 (Act 332) also protects original works from unauthorized reproduction and distribution. Using AI to edit an image, video or even a voice requiring permission is also considered copyright infringement. This means anyone could be charged for AI copyright, such as generating a programmatic advertisement through the likeness or voice of an influencer — without permission. It offers a legal remedy to assist the protection of creative works from duplication or creation by artificial intelligence.

There are other relevant provisions within the Penal Code (Act 574) particularly in relation to crimes committed using AI since this wider law of the land would also need to address such issues. To constitute a criminal offense, false statements made or published concerning another man with the intent to harm his reputation is prescribed under Section 499, namely that defamation. If AI generates fake endorsements or other confusing statements about a person, this could fall under false endorsement — and harming someone's reputation can be damaging to the truth. Under section 500 of the Penal Code, further characterisation of defamation is given and allows for those subjected to such harm by AI-driven defamation to seek remedy.

Another aspect is that the issue of criminal intimidation also falls under Section 503 of the Penal Code, which is where a threatening to harm a person’s reputation or person. Content with deepfake of threatening or blackmailing someone—for example, creating something obscene about them—could also fit into this category if the intention is to intimidate or threaten someone. Gestures or words intended to insult the modesty of a person are also criminalized under Section 509 of the Penal Code, and this could easily apply to deepfakes that depict an Individual in an offensive manner.

Defamation Act of 1957 contains the provisions/guidelines for civil aspects of defamation as well. Where artificial intelligence outputs harm someone’s reputation, this allows victims to pursue civil remedies for instance damages due to reputational harm. With the advent of deepfake and AI-manipulated content that has begun to impact public figures and influencers, this act is a crucial avenue for defending reputation.

Nonetheless, the technology underlying AI is only developing further, potentially requiring additional precision and exactness in the legal framework by which it operates to address what market power theory may not be able to properly capture, namely the distinct features of AI manipulation. We need to strengthen these laws if we are to protect people adequately and not run the risk of eroding public confidence in the digital spaces where AI-generated content is clearly becoming a larger presence. Lawmakers, technology developers and the general public need to work together now more than ever before in order to come up with ways to balance innovative progress with strong ethical and legal protections for well-being in this new era of artificial intelligence.

Challenges from a Malaysian Legal Perspective

Malaysia has experienced a very fast development with regards to AI technology that has outpaced the drafting of specific laws and legislation, bringing forth large legal and ethical shortcomings. The scope of existing legislation is very narrow without the comprehensiveness needed to cover the varied dimensions of crimes connected with AI. This limitation presents a very huge obstacle to law enforcers who detect, track, and prosecute individuals misusing the AI technology.

Such lack of specific legislation on AI and the growing number of cybercrimes associated with this technology point out a critical issue in Malaysia's legal landscape. The existing legislation was never designed to tackle the unique features that AI presents, such as its capacity for autonomous decision-making, adaptive learning, and self-enhancement. As such, ascribing the element of culpability over AI-related offenses is an immensely multi-dimensional challenge. It is ambiguous to determine the accountability, whether it is the user who misuses the AI, the developer who created it, or the AI system itself, which is high in autonomy according to its operating parameters (Baldi & Oliveira, 2022). This ambiguity creates liabilities that make crimes associated with AI very hard to prosecute, where traditional legal principles may not always fit neatly into this new and complex technology.

Moreover, the speed at which development is happening in AI greatly outpaces the ability of existing laws to adapt, thereby creating a disconnect between legal frameworks and technological development. This mismatch in progress leaves a number of parties vulnerable—be it influencers or consumers. In the case of influencers, they stand a chance of being publicly misled and having their reputation damaged through manipulation of images or utterances using AI without permission from them. Similarly, AI-generated content in digital ads may mislead consumers into believing that such an endorsement or testimonial is wholly fabricated.

The lack of AI legislation opens opportunities to manipulate content in social media advertising for financial gain at the expense of authenticity. Deepfake technologies can create synthetic but realistic-looking endorsements by influencers or public figures, deceiving consumers into trusting a product or service under false pretenses. This exploitation, therefore, deprives online platforms of public trust, and it is becoming increasingly difficult to tell what is real and what has been manipulated by AI.

There is protection afforded under the current legal framework, which consists of the Communications and Multimedia Act 1998, the Personal Data Protection Act 2010, and the Penal Code. These are the laws presently providing protection, though they were not drafted with the manipulability brought about by AI in mind. For example, the Communications and Multimedia Act speaks to the improper use of network facilities but does not make provisions for specific challenges presented by AI, such as automated content creation. Similarly, personal data is safeguarded under the Personal Data Protection Act, although it lacks clear provisions on how to treat cases involving AI-generated content which may violate privacy or libel persons.

These challenges have hence driven the need for reform in Malaysia to have comprehensive legislation that shall deal with the distinctive features of AI. So long as specific laws and regulations are not in place, the Malaysian legal system will always fail to protect individuals against crimes that can be committed through AI. A regulatory framework of AI by policymakers needs to examine the ethical, legal, and social implications of AI technology. The framework should comprise liability, transparency, and accountability guidelines for AI applications, more so in the fields where technology can be applied with easy harm, such as in social media and digital advertising.

Conclusion

Malaysia has grappled with the escalating misuse of Artificial Intelligence, especially in digital spaces. The government must proactively ensure the creation of a responsible and secure AI ecosystem in the face of this challenge. The first goal is to create a comprehensive legal framework customized for artificial intelligence. That would be a framework regulating the use of AI, in consideration of clear guidelines on accountability, liability, and ethical standards, hence allowing the possibility of regulation while at the same time preventing abuse. This legal framework is greatly important to assure responsible usage of AI technology in different fields. Besides legislation, skills on the side of law enforcement need improvement, too. Specialized training in AI technologies and digital forensics would empower law enforcement personnel with the necessary expertise to effectively enforce AI-related laws. Malaysia needs to invest in its technological infrastructure. With advanced tools and systems in place, the detection and monitoring of AI-generated content in real time would help combat AI-related threats. It would increase the ability of the country to deal with fast-changing developments in AI and result in a much safer digital environment for all.

In conclusion, with the development of specific AI legal framework, enhancement of skills in law enforcement, and technological infrastructure, Malaysia will be able to protect individuals from risks related to AI while supporting responsible AI innovation. These are very crucial steps toward building public trust and ensuring that AI contributes positively to Malaysia's progress.

References

Amerini, I., Barni, M., Battiato, S., Bestagini, P., Boato, G., Bonaventura, T. S., Bruni, V., Caldelli, R., Natale, D., Nicola, D., Guarnera, L., Mandelli, S., Luca, M. G., Micheletto, M., Montibeller, A., Orru, G., Ortis, A., Perazzo, P., Salvi, D., & Tubaro, S. (2024). Deepfake media forensics: state of the art and challenges ahead. *ArXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2408.00388

Baldi, V., & Oliveira, L. (2022). Challenges to incorporate accountability into artificial intelligence. *Procedia Computer Science*, *204*, 519–523. https://doi.org/10.1016/j.procs.2022.08.063

Chauhan, S., & Thakur, S. (2023). A study on consumers' perspective towards social media marketing during Covid-19. *Interantional Journal Of Scientific Research In Engineering And Management*, *07*(02). https://doi.org/10.55041/ijsrem17685

Communications and Multimedia Act 1998 (Act 588)

Copyright Act 1987 (Act 332)

Defamation Act 1957

Dubey, N. (2024). The implementation of artificial intelligence and its future potential. *Interantional Journal Of Scientific Research In Engineering And Management*, *08*(04), 1–5. https://doi.org/10.55041/ijsrem31925

Faraasyatul 'Alam, G., Wiyono, B. B., Burhanuddin, B., Muslihati, M., & Mujaidah, A. (2024). Artificial intelligence in education world: opportunities, challenges, and future research recommendations. *Fahima*, *3*(2), 223–234. https://doi.org/10.54622/fahima.v3i2.350

H Patel, U., & Gera, K. (2024). Biometric security systems enhanced by ai: exploring concerns with ai advancements in facial recognition and other biometric systems have security implications and vulnerabilities. *International Journal of Innovative Science and Research Technology (IJISRT)*, 2078–2082. https://doi.org/10.38124/ijisrt/ijisrt24jun1510

Mathew, A. (2024). Artificial intrusions: the dark art of ai exploitation. *International Journal of Computer Science and Mobile Computing*, *13*(8), 54–59. https://doi.org/10.47760/ijcsmc.2024.v13i08.006

Penal Code (Act 574).

Personal Data Protection Act 2010 (Act 709).

Shrivastava, A. (2024). Artificial intelligence (ai): evolution, methodologies, and applications. *International Journal for Research in Applied Science and Engineering Technology*, *12*(4), 5501–5505. https://doi.org/10.22214/ijraset.2024.61241