Asian Journal of Law and Policy
Vol 5 No 3 (December 2025) eISSN: 2785-8979

Addressing Child Exploitation via Deepfake Technology: Evaluating Malaysia's Legal Framework

Phaik Nee Tan
Faculty of Law, Multimedia University, Malaysia
1211101388@student.mmu.edu.my
ORCID iD: 0009-0003-9445-4475
(Corresponding author)

Manique AE Cooray
Centre for Law and Technology, Faculty of Law, Multimedia University, Malaysia
manique.cooray@mmu.edu.my
ORCID iD: 0000-0003-3066-0985

ABSTRACT

The rapid development in artificial intelligence (AI) has led to the proliferation of deepfake technology. The advancement of deepfake technology has posed significant risks, particularly its significant threats to children through exploitation. This paper aims to examine the effectiveness of Malaysia's current legal framework in tackling deepfake child pornography and to identify existing legal gaps. Despite the severe implications of deepfakes in facilitating child pornography and other forms of abuse, Malaysia currently lacks specific laws to address these pressing issues. Thus, this paper delves into effective legislative measures to tackle deepfake-related crime through a comparative analysis of the legal approaches in the United Kingdom, Singapore, South Korea and the European Union. By identifying the key provisions and case laws in these jurisdictions, this study proposes to reform Malaysia's outdated laws to criminalise the parties liable for the crime and point up the need to adopt a robust legal framework to safeguard victims and deter potential offenders.

Keywords: Deepfakes; Artificial intelligence; Child exploitation; Malaysian legislation

Received: 4 February 2025, **Accepted:** 30 June 2025, **Published:** 1 December 2025

(2025) 5(3) Asian Journal of Law and Policy 199–224
https://doi.org/10.33093/ajlp.2025.12

Published by MMU Press. URL: https://journals.mmupress.com/ajlp

1. Introduction

In recent years, the rapid development of artificial intelligence (AI) has revolutionised various industries and created unprecedented opportunities and innovations. One of the notable advancements in this field is deepfake technology. The word 'deepfake' is a combination of 'deep learning' and 'fake', and it refers to highly realistic video or image content produced through deep learning algorithms.[1] The term gained widespread attention in 2017 when a group of Reddit users posted fake sexual content where the faces of female celebrities were superimposed onto the bodies of adult performers using AI technology.[2]

By using the technology, anyone can create a highly realistic face of a person who does not exist in the world. The technology allows the alteration of a person's facial appearance, such as identity swap, in a video with a high level of realism.[3] These fabricated videos, audio, or images are crafted to appear and sound authentic. As AI technology continues to advance, the amount of data required to produce increasingly convincing forgeries is diminishing. The defining characteristic of deepfakes lies in their use of machine learning to replicate facial expressions with a natural fluidity that once required extensive and manual effort.[4]

One group particularly vulnerable to deepfake technology is children. In a recent case involving OpenAI, its technology was found to facilitate the spread of video and audio deepfakes by collecting, storing, and analysing vast amounts of highly personalised data, and the detection is challenging. The victims of deepfake technology are not limited to non-consenting adults only. The issue has also extended to include minor children, thus raising concerns about exploitation and abuse.[5]

In Malaysia, a 'child' is legally defined as any person under the age of 18, as stated in Section 2(1) of the Child Act 2001. According to the United Kingdom (UK) Home Office, child sexual exploitation is a form of abuse in which an individual or group leverages a power imbalance to coerce, manipulate, or deceive a child or young person under the age of 18 into engaging in sexual activity either in return for something the victim desires or for the perpetrator's benefit. Importantly, child sexual exploitation does not always involve physical contact, it can also take place through digital means using technology.[6]

---

[1] Md Shohel Rana and others, 'Deepfake Detection: A Systematic Literature Review' (2022) 10 Institute of Electrical and Electronics Engineers Access <https://doi.org/10.1109/ACCESS.2022.3154404>.

[2] Dilrukshi Gamage and others, 'Are Deepfakes Concerning? Analyzing Conversations of Deepfakes on Reddit and Exploring Societal Implications' [2022] 103 Computer Human Interaction 1 <https://doi.org/10.1145/3491102.3517446>.

[3] Felix Juefei-Xu and others, 'Countering Malicious DeepFakes: Survey, Battleground, and Horizon' (2022) 130 International Journal of Computer Vision 1678 <https://doi.org/10.1007/s11263-022-01606-8>.

[4] Egor Zakharov and others, 'Few-Shot Adversarial Learning of Realistic Neural Talking Head Models' [2019] Institute of Electrical and Electronics Engineers /Computer Vision Foundation International Conference on Computer Vision 9458 <https://doi.ieeecomputersociety.org/10.1109/ICCV.2019.00955>.

[5] PM et al v OpenAI LP et al, 3:23-cv-03199.

One approach to addressing the exploitation of children through deepfake technology is the introduction of specific legislation aimed at regulating its use. Such laws should comprehensively cover all aspects of deepfake content. For example, Virginia's deepfake laws primarily focus on deepfake pornography and revenge porn.

Accordingly, this paper seeks to examine the potential of Malaysia's existing legal framework to combat child exploitation facilitated by deepfake technology. The paper also explores the legal approaches adopted by other countries such as the UK, Singapore, and South Korea, and an international organisation, the European Union. The UK and South Korea have established a comprehensive legal framework to address crimes involving deepfake technology, particularly sexually explicit deepfakes. In contrast, Singapore, like Malaysia, has not yet introduced specific laws to tackle such crimes. Instead, it relies on existing legislation to address these issues. Lastly, effective strategies will be proposed to curb such exploitation.

2. Research Methodology

This paper adopts a qualitative research methodology to analyse and evaluate the existing law in Malaysia and other jurisdictions. This paper relies on doctrinal analysis by examining relevant legislations and amendments in Malaysia relating to deepfake technology and child exploitation. The study draws upon information from journal articles, research papers. and news articles.

Besides that, comparative legal analysis is conducted by analysing the legal frameworks in other jurisdictions such as the UK, Singapore, South Korea, as well as international frameworks such as the European Union's AI Act. The comparison between the jurisdictions highlights the inadequacies in Malaysia's legal system regarding the regulation of deepfake technology. Thus, reforms are proposed based on the findings from the comparative analysis.

3. Malaysia's Legal Framework on Child Exploitation

Deepfake technology represents a modern tool used to facilitate one of the world's oldest crimes. Despite that deepfake materials and the applications to create them are readily accessible in Malaysia, there are currently no specific regulations and limitations governing its usage. In this context, child pornography is the most closely associated offence with the deepfake child pornography crime, which is addressed under various Malaysian statutes and legal provisions. This section will primarily rely on the prohibition of child pornography as well as obscene and indecent content under Malaysian law.

[6] United Kingdom Home Office, 'Child exploitation disruption toolkit' (2022) <https://www.gov.uk/government/publications/child-exploitation-disruption-toolkit/child-exploitation-disruption-toolkit-accessible>.

3.1 Sexual Offences Against Children Act 2017

In cases of child sexual exploitation in Malaysia, the Sexual Offences Against Children Act 2017 (SOCA) is the primary legislation that will be invoked. However, this Act does not explicitly address offences involving deepfake technology.

3.1.1 Definition of Child Pornography Under SOCA

The issue of child pornography is outlined under Part II of the SOCA. Section 4(a) of SOCA defines 'child pornography' as any representation, whether visual, audio, written or any of their combination, produced by any means, including electronic, mechanical, digital, optical, magnetic or manual methods, showing a child engaging in sexually explicit conduct. The inclusion of the phrase 'including but not limited to' in this provision allows flexibility in applying this provision to child intimate materials created using deepfake technology.

3.1.2 Offences Under SOCA

The creation of deepfakes child pornography can be separated into two stages, which are the preparation stage and the creation stage itself. SOCA criminalised any individual who is involved in the creation, production, or direction of child pornography. Such a person is punishable under Section 5 of SOCA by up to 30 years of imprisonment and a minimum of six strokes of whipping.

Additionally, the offender who is caught in the preparation stage prior to the actual creation of child pornography will face a lighter penalty under Section 6 of SOCA for up to 10 years of imprisonment and may also include whipping.

In addition to involvement in the creation or production of child pornography, any individual who distributes such material by way of exchanging, publishing, printing, reproducing, selling, importing, exporting and otherwise commits an offence. Likewise, it is also an offence when the individual receives the materials by way of obtaining, collecting, or seeking any child pornography, or participates in or profits from a business related to any child pornography.

Committing these offences will be held liable under Section 8 of SOCA and is punishable with imprisonment up to 15 years and a minimum of three strokes of whipping. This section may be invoked when the deepfake child intimate materials are distributed, obtained, or used by the perpetrators for financial gain. By referring to the illustration provided under the same provision, an administrator of a website displaying child pornography is considered guilty of an offence. Similarly, this provision may be applied when the administrator of an online platform makes children's deepfake intimate images or videos available. Therefore, it implies that a website administrator who omits to remove child pornography content will also be held liable under this section.

Besides that, harsher punishment is imposed on the individual who distributes child pornography to a child as stated under Section 9 of SOCA, including selling, letting to hire, distributing, exhibiting, advertising, transmitting, promoting, etc, the materials to a child. This offence is punishable with imprisonment up to 15 years and a minimum of five strokes whipping.

Despite the production and distribution of child pornography, any individual who has access, possesses, or has control over any child pornography commits an offence under Section 10 of SOCA and may face imprisonment for a term up to five years or to a fine not exceeding RM10,000, or to both.

Not only that, any person who has knowledge of the commission or intention to commit the offence of creating or distributing deepfake content and fails to report it to the officer in charge of the nearest police station commits an offence under Section 19 of SOCA. This provision may hold adults around the victim liable if they are aware of such content but fail to report it.

3.1.3 Limitations of SOCA

These provisions could possibly be applied to criminalise perpetrators involved in the creation, direction, distribution, or possession of deepfake intimate images or videos featuring a child's face or voice. While these provisions offer some flexibility in addressing deepfake child pornography, the statute fails to include deepfake-generated content as part of child pornography. Thus, the provisions still fall short of explicitly recognising and criminalising the use of deepfake technology as a stand-alone offence.

3.2 Communications and Multimedia Act 1998

In Malaysia, the Communications and Multimedia Act 1998 (CMA) is one of the legislations that may possibly address deepfake issues.[7] The CMA serves as the main legislation that governs the communications and multimedia industry and fosters a robust applications environment for end users. The Act ensures information security as well as the reliability and integrity of networks.

3.2.1 Prohibition on Providing Offensive Content Under Section 211 of CMA

Deepfake pornography might be categorised as offensive content in CMA. Section 211 of CMA sets out five categories of offensive content, namely indecent, obscene, false, or offensive online content. The prohibition against content application service provider or their user in providing offensive content under Section 211(1) of CMA requires the element

[7] Zec Kie Tan and others, 'Individual Legal Protection in the Deepfake Technology Era' (International Conference on Law and Digitalization 2023) <https://doi.org/10.2991/978-2-38476-154-8_7>.

of mens rea, which is the intention of the offender to annoy, abuse, threaten, or harass any person by providing the content, which is indecent, obscene, false, or offensive.[8]

Any offender who fulfils the actus reus and mens rea is violating the law and shall be punishable by a fine of RM50,000 maximum or imprisonment for a term up to one year or both. Additionally, a continuing offence after conviction incurs a further fine of RM1,000 each day the offence persists.

The scope of this provision is broad enough to encompass the dissemination of deepfake intimate materials. However, it is limited to regulating the distribution of deepfake content through online platforms and does not extend to criminalising the creation of deepfakes. The legal protections provided under this section are viewed as insufficient, as there is no specific legal framework designed to regulate the deepfake technology itself.[9]

3.2.2 Improper Use of Network Facilities or Network Service Under Section 233 of CMA

Section 233 of CMA can be invoked in cases involving the creation and dissemination of deepfake child pornography. The provision makes it an offence for any individual to make, create, solicit, and initiate the transmission of any communication that is obscene, indecent, false, menacing, or offensive with the intention to annoy, abuse, threaten, or harass another person using network facilities, network service, or application services. This applies regardless of whether the conduct is continuous or isolated, and regardless of whether the perpetrator conceals their identity.

In the context of deepfake child pornography, the perpetrator who fabricates and shares such content depicting a child would fall within the scope of this offence. The false and indecent nature of deepfake pornography involving children clearly aligns with the language of Section 233 of CMA, particularly with the intention to degrade or exploit the child.

Another significant aspect provided in Section 233(2)(a) is that it extends the liability towards the individual who does not directly involve in the creation of the deepfake child pornography but who provides the obscene material for commercial purposes or allows the use of a network service or applications service under their control for such purpose. This provision may apply to online platform administrators, website operators, or content hosts who facilitate access or fail to remove deepfake child pornography from their services.

---

[8] Ammar Abdullah Saeed Mohammed and Nazli Ismail Nawang, 'Offensive Content on The Internet: The Malaysian Legal Approach' Spec Ed (2019) 5(2) International Journal of Innovation, Creativity and Change <https://www.ijicc.net/images/Vol5iss2_/24_Mohammed_P367_2019R.pdf>.

[9] Jin Yang Ng and others, 'Enhancing Deepfake Detection for Public Awareness, Law Enforcement and Legal Verification' (International Conference on Information Technology Research and Innovation 2024) <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10699122>.

Upon conviction, the perpetrators may be punished with a fine not exceeding RM50,000 or to imprisonment for a term not exceeding one year, or to both. Additionally, if the offence continues after conviction, the perpetrator is liable for a further fine of RM1,000 for each day.

3.2.3 Limitations of CMA

CMA does not criminalise the individuals who upload, download, receive, view, or possess obscene content.[10] Malaysia Internet Service Providers are not required to remove or report offensive content related to child sexual abuse and exploitation.[11]

Furthermore, the CMA lacks specific definitions of pornography or obscenity, and its provisions do not align with international standards.[12] These definitions will be further discussed below under the Content Code.

4. The Malaysian Communications and Multimedia Content Code 2022

The terms commonly used in CMA, such as obscene, indecent, and false, are explained under the Content Code.

The Content Code was first introduced by the Malaysian Communications and Multimedia Commission (MCMC) in 2004, and it has been reviewed and revised throughout the years. The Content Code 2022 was officially registered by MCMC and came into effect on 30 May 2022. The Content Code prohibits Internet Service Providers, Internet content hosts, online content developers, online content aggregators, and link providers in Malaysia, which are also referred to as Code subjects, from providing and distributing illegal content, such as that is indecent, obscene, menacing, and offensive in nature.

4.1 Definition of 'Indecent', 'Obscene', and 'False' Under Content Code

The term 'indecent content' is defined in Section 2.0 of Part 2 of the Content Code as material that is offensive, morally inappropriate, and contrary to current accepted societal standards. This includes nudity and sexual content. However, there is an exception that non-sexual depictions of nudity related to art, information, or science are permitted as long as they are not excessive or explicit.

---

[10] Juriah Abdul Jalil, 'Combating Child Pornography in Digital Era: Is Malaysian Law Adequate to Meet the Digital Challenge?' (2015) 23(S) Pertanika Journal of Social Sciences and Humanities 137 <http://www.pertanika.upm.edu.my/resources/files/Pertanika%20PAPERS/JSSH%20Vol.%2023%20(S)%20Oct.%202015/11%20JSSH%20Vol%2023%20(S)%20Oct%202015_pg137-152.pdf>.

[11] Mubarak Rahamathulla, 'Cyber Safety of Children in the Association of Southeast Asian Nations (ASEAN) Region: A Critical Review of Legal Frameworks and Policy Implications' (2021) 4 International Journal on Child Maltreatment: Research, Policy and Practice 375–400 <https://doi.org/10.1007/s42448-021-00087-5>.

[12] Haezreena Begum bt Abdul Hamid, 'Combatting Sexual Cyberviolence Against Women in Malaysia' [2022] 3 Malayan Law Journal ccxxx <https://advance.lexis.com/api/permalink/cc1419e9-f0ee-40b1-aa47-e16776b41658/?context=1522468>.

Besides, 'obscene content' is defined as material that elicits feelings of disgust due to its lewd portrayal and is essentially offensive to the prevailing notion of decency and modesty. Such content has the potential to negatively influence and corrupt the minds of those who are easily swayed. The test for obscenity is whether the Content has the tendency to deprive and corrupt those whose minds are open to such communication. The examples of obscene content include explicit sex acts or pornography, child pornography, and sexual degradation. The term 'child pornography' in this context shall carry the definition provided under Section 4 of SOCA 2017.

Under section 7.0 of the same Part, 'false content' refers to false material or incomplete information that is likely to mislead and must be avoided.

Deepfake intimate materials involving children fall within the definition of indecent, obscene, and false content. Even in the absence of physical abuse, the creation and provision of pornographic content using a fabricated depiction of a child is highly concerning. Such content is capable of misleading the public into believing it depicts a real event.

Pornography alone is widely regarded as morally inappropriate and unacceptable by current accepted standards behaviour. This concern is significantly heightened when it involves minors. No child should ever be depicted in this form of content. Furthermore, deepfake content involving children evokes feelings of disgust and is inherently offensive to the prevailing notion of decency and modesty.

4.2 Limitations of Content Code

Although the Content Code may potentially address deepfake child pornography, it does not apply to ordinary Internet users as they are not included as Code subjects. The Content Code was designed for industry self-regulation and only applies to industry actors such as Internet Service Providers, Internet content hosts, online content developers, online content aggregators, and link providers. The applicability of the Code will be limited in its practical impact as deepfakes content creators are typically individuals who fall outside the scope of the Code's framework.

Furthermore, Part 1, Section 6.2 of the Code explicitly states that compliance with its provisions is voluntary. This suggests that the Code is lacking legally binding effect. Nonetheless, Internet users were expected to adhere to proper Internet etiquette in line with the self-regulation principles promoted by the Content Code.[13]

5. Penal Code

The offences and penalties outlined in the Penal Code (PC) are not specifically intended to protect only child victims. The law does not prohibit the crime in its early stage, such as the

[13] Mahyuddin Daud, Juriah Abd Jalil, 'Protecting Children Against Exposure to Content Risks Online in Malaysia: Lessons from Australia' (2017) 33(1) Malaysian Journal of Communication 115 <https://doi.org/10.17576/JKMJC-2017-3301-08>.

creation of the obscene materials, but rather focuses on preventing the distribution of such content.

Particularly, the distribution of obscene objects is prohibited under Section 292 of PC. Distribution in this context refers to selling, letting to hire, distributing, making, or having in his possession any obscene object. In addition, importing, exporting, conveying, or taking part in or receiving any profits from the business involving obscene objects is also prohibited. Those found guilty of any of these offences may face imprisonment for up to three years or with fine, or both.

On top of that, under Section 293 of PC, anyone who distributes or provides the obscene objects to individuals under the age of 20 will face harsher penalties, namely punishment of imprisonment for a term not exceeding five years or a fine or both.

5.1 Limitations of Penal Code

Similar to CMA, PC does not explicitly address deepfake-related crimes nor their creation. In some instances, creators of deepfakes child pornography produce such content not for public distribution but for personal sexual gratification or other private purposes. As a result, leaving the creation stage unregulated creates a loophole that makes it difficult to penalise this category of offenders in cases involving deepfake technology.

In addition, the adequacy of the penalties under Section 292 and Section 293 as a deterrent for modern crimes such as the distribution of deepfake content is questionable. The anonymity provided by the technology, coupled with the ease of disseminating deepfake content, requires harsher punishment to effectively to deter the offenders and underscore the seriousness of such crimes.

6. Personal Data Protection Act 2010

The only legislation addressing privacy law in Malaysia is the Personal Data Protection Act 2010 (PDPA).

The personal data protection principles are outlined in Division 1 of the PDPA, specifically under Section 5 to Section 12, which encroach the general principle, the notice and choice principle, the disclosure principle, the security principle, the retention principle, the data integrity principle, and the access principle.

By looking into Section 6(1) of PDPA, this section makes it an offence to use the personal data of the data subjects without their consent. Aside from that, subsection (3) provides that the personal data shall also be processed only for a lawful purpose directly related to an activity of the data user, and it must be necessary, relevant, and not excessive for that purpose.

Under subsection (1), it appears that if the victim of deepfake child pornography consented to the use of their face or voice in the creation of such content, the perpetrator

may not fall within the scope of the section. However, it must be emphasised that the use of personal data in the creation of deepfake child pornography is not a lawful purpose. As such, the creator would still violate the law.

6.1 Limitations of Personal Data and Protection Act 2010

It can be argued that the current PDPA does not adequately safeguard the privacy rights of the data subject as its scope is limited to information related to commercial transactions as provided under Section 2(1) of the PDPA.[14] As a result, it is recommended that a separate law should be introduced to protect personal data from being misused by private individuals due to the fact that the majority of deepfake abuse is perpetrated by individuals rather than commercial entities.[15]

Furthermore, it must be determined that the personal data, such as the face and voice of the children, are processed for the creation of the deepfake video without the consent of the data subject. However, it raised enforcement difficulties for how the authorities should determine whether consent was obtained from the victim for the personal data used in deepfake creation.

7. Child Act 2001

The Child Act is not discussed in this paper because its offences and protective provisions primarily focus on physical abuse rather than technology-facilitated abuse like deepfake child pornography. Moreover, for an offender to be prosecuted under the Child Act, the victim must be under the care, custody, or control of the offender.[16] This element is often absent in cases involving digitally manipulated content.

7.1 Challenges in Enforcing and Implementing

7.1.1 Lack of Specific Laws (Jurisdictional Challenges)

In Malaysia, there is a significant gap in our legal framework for dealing with the issue of deepfakes created content. Even more alarming is the lack of specific laws designed to safeguard children from deepfake-generated intimate materials.

---

[14] Shao Zheng Chong and Chee Ying Kuek, 'Facial Recognition Technology in Malaysia: Concerns and Legal Issues' (International Conference on Law and Digitalization 2022) <https://doi.org/10.2991/978-2-494069-59-6_10>.

[15] Zec Kie Tan (n 7).

[16] Mahmud Abdul Jumaat, 'SWOT Analysis on Child Sexual Abuse Framework Under Malaysia's Sexual Offences Against Children Act 2007' (2023) 40(1) INSAF The Journal of the Malaysian Bar 11 <https://www.malaysianbar.org.my/cms/upload_files/document/INSAF%20Vol%2040%20No%201%20(June%202023).pdf>.

The relevant laws are dispersed across various legislations. This may lead to difficulties in aligning the enforcement of laws to address the form of misuse of deepfake technology involving children. For example, while the term 'child pornography' is defined under SOCA, it lacks a clear definition in CMA. Additionally, the CMA does not provide definitions for obscenity and indecency. The terms were only outlined in the Content Code. However, the Content Code merely served as a guideline for self-regulation by online content providers. It does not have binding legal effect and applies only to Internet Service Providers (ISPs) that have consented to be bound by it and does not extend to all Internet users.[17]

One recent case involving AI-generated deepfake pornography caused a huge public uproar. A 16-year-old student from Foon Yew High School was arrested for allegedly creating and selling pornographic images of his schoolmates and school alumni using deepfake technology. The suspect reportedly obtained the victims' photos from social media. The fabricated images were sold at RM2 each. Among the identified victims, some of them were as young as 12 or 13 years old.

Authorities were investigating the case under Section 233 of the Communications and Multimedia Act for sharing offensive and inappropriate content, as well as Section 292 of the Penal Code, which prohibits the sale, distribution, or circulation of obscene materials.[18]

This case shows a critical gap in Malaysia's legal framework, as there is currently no specific legislation addressing crimes involving deepfakes. As a result, the authorities are relying on scattered general provisions that are not directly targeting at deepfakes crime.

7.1.2 Difficulties in Identifying Deepfake Creators (Anonymity)

Another significant challenge for authorities in combating deepfake-related crime is tracking down criminal activity[19] due to the anonymity offered by digital platforms and tools. Deepfake creators usually hide behind pseudonyms or utilise tools like VPNs to mask their identities. The child pornography offenders have formed communities on 'Dark Web', a platform where they can anonymously share and engage in child sexual abuse. As defined by Oxford Dictionary, Dark Web is a segment of the World Wide Web that can only be accessed through specialised software that enables users and website operators to remain anonymous and untraceable. Thus, when deepfake crimes are committed anonymously, it becomes challenging for the authorities to track down the perpetrators. A broad range of

[17] Jin Yang Ng (n 9).

[18] Venesa Devi, 'Johor Teenager Nabbed for Allegedly Creating, Selling Lewd AI Pics of Schoolmates' *The Star* (Johor Baru, 9 April 2025) <https://www.thestar.com.my/news/nation/2025/04/09/johor-teenager-nabbed-for-allegedly-creating-selling-lewd-ai-pics-of-schoolmates>.

[19] Anuragini Shirish and Shobana Komal, 'A Socio-Legal Inquiry on Deepfakes' (2024) 54(2) art 6 California Western International Law Journal 517 <https://scholarlycommons.law.cwsl.edu/cwilj/vol54/iss2/6>.

digital tools is necessary to penetrate the anonymity, conduct investigations, identify those responsible, and terminate the involved websites.[20]

7.1.3 The Cross-Border Nature of Online Exploitation

In the digital realm, another major challenge in addressing deepfake content is the absence of geographical boundaries. This issue arises when a perpetrator residing in country A creates deepfake content targeting a victim in country B. The situation becomes even more complex if the content is uploaded to a platform operated from country C. There is an absence of standardised offences across different countries' legal frameworks as conduct constitutes a crime in one jurisdiction may not be treated as such in another. Besides that, there is no mandatory legislation requiring the states or the companies to cooperate by providing necessary data to foreign authorities. Law enforcement authorities often face difficulties when the requested information is controlled by ISPs based abroad, as they may refuse to comply with the local legislation of the enforcing authority.[21] Therefore, it came to the conclusion that the lack of harmonised international regulations and cooperative mechanisms exacerbates the problem and hinders the efforts to hold the perpetrators accountable.[22]

8. Findings and Analysis

8.1 United Kingdom

In recent years, the UK has introduced new legislation and proposed amendments to its existing laws to address crimes arising from advancements in technology. The distribution of deepfake intimate images was initially criminalised under the Online Safety Act 2023 (OSA 2023). However, this legislation did not impose punishment on the creator of the deepfake content. Thus, in a press release issued in April 2024, the UK government announced that individuals involved in the creation of sexually explicit deepfakes would soon face prosecution under the newly revised Criminal Justice Bill.[23] This amendment builds upon the existing offence of sharing deepfake intimate images, which was first introduced as a priority offence under the OSA.[24]

---

[20] Abigail Olson, 'The Double-Side of Deepfakes: Obstacles and Assets in the Fight Against Child Pornography' (2022) 56(2) art 8 Georgia Law Review 865 <https://digitalcommons.law.uga.edu/glr/vol56/iss2/8>.

[21] Mohamed Hassan Mekkawi, 'The Challenges of Digital Evidence Usage in Deepfake Crimes Era' (2023) 3(2) Journal of Law and Emerging Technologies 176 <https://doi.org/10.54873/jolets.v3i2.123>.

[22] 'Deepfakes and Online Scams: Navigating Legal Issues in Hong Kong and Singapore' (*withersworldwide*, 12 June 2024) <https://www.withersworldwide.com/en-gb/insight/read/deepfakes-and-online-scams-navigating-legal-issues-in-hong-kong-and-singapore>.

[23] Ministry of Justice and Laura Farris, 'Government Cracks Down on 'Deepfakes' Creation' (*GOV.UK*, 16 April 2024) <https://www.gov.uk/government/news/government-cracks-down-on-deepfakes-creation>.

[24] 'Criminalising Deepfakes–The UK's New Offences Following the Online Safety Act' (*Herbert Smith Freehills Kramer*, 21 May 2024) <https://www.herbertsmithfreehills.com/notes/tmt/2024-05/criminalising-deepfakes-the-

At the outset, it should be clarified that neither the amendment nor the new law specifically addresses the deepfake pornography involving children. Instead, the current legal reforms take a general approach to sexually explicit deepfake content without distinguishing offences based on the age of the victim.

8.1.1 Amendment to Criminal Justice Bill

The creation of sexually explicit deepfakes has been criminalised through amendments to the Criminal Justice Bill by the introduction of a new offence under Section 66AD for 'faking intimate photographs or films using digital technology'. Under this provision, it becomes a crime when a person intentionally produces or designs an image or film that appears to depict another individual in an intimate stage using computer graphics or other digital technologies.

The provision provides three scenarios under which creating such deepfake pornography constitutes a criminal offence. Firstly, the image or film is created for sexual gratification creator or another person. Secondly, even if the deepfake pornography is not distributed, the mere act of fabricating explicit content with the intent to cause alarm, distress, or humiliation to the victim is punishable. Thirdly, the offender created the deepfake content showing the victim's genitals[25] or the victim is in an intimate state[26] with the intention to distribute it.

Despite the offence, the perpetrators may raise a defence under Section 66AD(2) of the Criminal Justice Bill (Amendment) if they had a reasonable excuse for creating or producing the image or film, or that the victim had consented to its creation.[27]

8.1.2 Online Safety Act 2023

The OSA 2023, which took effect on 31 January 2024, introduces four new offences to the Sexual Offences Act 2003 focusing on the distribution of deepfake pornography. Under the OSA 2023, it is unlawful to share or threaten to share intimate images, including deepfakes, of individuals without their consent. These newly established offences are outlined in Section 187 and Section 188 of OSA 2023 and will be incorporated into SOA 2003 as Section 66A to Section 66D.

Before delving into the offences, the terms 'photograph' and 'film' are interpreted under subsection (3) to subsection (5) of Section 66A of SOA 2003. For the purposes of Section 66A to Section 66D, 'photograph' encompasses both negative and positive forms, whereas 'film' refers to any moving image. On top of that, photograph or film also includes image created or modified through computer graphics or other means that resemble photographs or films.

uks-new-offences-following-the-online-safety-act>.

[25] Sexual Offences Act 2003, s 66A.

[26] Sexual Offences Act 2003, s 66B.

[27] Criminal Justice Bill (Amendment), 66AD (2).

The interpretation effectively includes deepfake intimate images and videos within the scope of the Act.

Looking into the offence, Section 66A makes it a crime for a person to intentionally send or share a photograph or film of another person's genitals with the intent to cause alarm, distress, or humiliation to the victim, or for the purpose of gaining sexual gratification.

Under Section 66B, the perpetrator who shares or threatens to share an intimate photograph or film is committing an offence if the conduct falls under any of the three limbs. Firstly, the perpetrator intentionally distributes such content depicting the victim in an intimate state without their consent. Secondly, the perpetrator intends to cause alarm, distress, or humiliation to the victim. Thirdly, the perpetrator has done so to obtain sexual gratification for themselves or another person. Fourthly, it is also considered an offence if the perpetrator threatens to share the image or film of the victim in an intimate state, regardless of whether the perpetrator has the intention to put the victim in fear that the threat will be carried out.

While Section 66B criminalises certain acts related to the sharing of deepfake pornography, Section 66C provides specific exemptions where the act may not constitute an offence when certain conditions are met. Firstly, it would be a defence if the perpetrator can prove that the photograph or film was taken in locations that allow the public to access where the victim has no reasonable expectation of privacy. Secondly, the victim was, or the perpetrator believes that the victim was, voluntarily in an intimate state. Thirdly, the perpetrator reasonably believes that the photograph or film had been previously publicly shared with the victim's consent.

8.1.3 Summary of the United Kingdom's Legal Framework

In summary, the UK has a relatively comprehensive legal framework for tackling deepfake technology in the context of child exploitation. While the laws are not solely focused on protecting children, they still cover all deepfake intimate images, including those that involve minors. The creation and distribution of deepfake images and videos are punishable under both the OSA 2023 and the Criminal Justice Bill. As said by Laura Farris, the Minister for Victims and Safeguarding, "the creation of deepfake sexual images is despicable and completely unacceptable irrespective of whether the image is shared".[28]

8.2 Singapore

In November 2024, an incident was reported regarding the deepfake nude photos of Singapore Sport Schools students had been created and circulated by schoolmates.[29] Despite

[28] Christy Cooney, 'Creating Sexually Explicit Deepfakes to Become a Criminal Offence' *BBC News* (16 April 2024) <https://www.bbc.com/news/uk-68823042>

[29] Gabrielle Chan, 'Police Investigating Deepfake Nude Photos of Singapore Sports School Students' *The Straits Times* (Singapore, 13 November 2024) <https://www.straitstimes.com/singapore/police-investigating-deepfake-

incidents occurring, Singapore does not have specific laws addressing deepfake pornography. However, this issue can be addressed through various existing laws, including the Penal Code, the Protection from Harassment Act, and the Films Act.

8.2.1 Singapore Penal Code

Singapore does not have specific legislation to tackle the issue of sharing and creating deepfake materials. However, certain legal provisions cover offences and punishments related to the creation and distribution of intimate images and videos, which may include deepfakes. In cases involving a minor victim, an individual who produces deepfake pornography with the face of a person below the age of 16 could be charged under Section 377BH of the Singapore Penal Code (SPC) for intentionally producing child abuse material. This offence is punishable by up to 10 years imprisonment, or a fine, or caning. In addition, distributing child abuse material is an offence and the offender could face imprisonment not more than seven years and can also be liable to a fine or caning.

Moving on, Section 337BE of the SPC criminalises the distribution of intimate images without consent, including intentional distribution or threats to distribute intimate images or recordings. The penalties for this offence include imprisonment of up to five years, or a fine, or caning. However, this provision introduced in the 2020 SPC amendment was primarily designed to deal with "revenge pornography" rather than general pornography. This implies that if the deepfake pornography is created for revenge purposes, it might fall under this provision.

There are certain scenarios involving deepfake pornography that may allow the perpetrators to evade accountability. First, under the provision, a video is not constituted as an "intimate recording" if it has been altered to the extent that no reasonable person would believe it depicts the victim. Consequently, if the deepfake video is of poor quality and does not convincingly resemble the victim, even if it still causes humiliation to the victim, the distributor may not be held liable. Second, for the offence to be established, the distributor must believe that their actions are likely to harass or humiliate the victim. Therefore, if the perpetrator argues that they distributed the video without knowing the identity of the victim and had no reason to believe it would cause humiliation, the offence may not be substantiated.[30]

Besides, merely possessing intimate images or videos on the device, whether created by the perpetrator, will be criminalised under Section 377BD of the SPC.

nude-photos-of-singapore-sports-school-students>.

[30] Josh Lee, 'Poon Chong Ming: Fake Porn, Real Harm: Examining the Laws Against Deepfake Pornography in Singapore' *(LawTech.Asia*, 3 October 2022) <https://lawtech.asia/fake-porn-real-harm-examining-the-laws-against-deepfake-pornography-in-singapore/>.

8.2.2 Protection from Harassment Act 2014

The Protection from Harassment Act (POHA) may be invoked in cases where deepfake intimate images or videos are used to harass or cause distress to a victim. Victims can seek remedies such as Protection Orders, which require the perpetrator to cease any further harassment.

Similar to SPC, POHA does not specifically address the creation or distribution of deepfake intimate materials. Notwithstanding this, the provisions may still be applicable in certain deepfake pornography cases. For example, Section 3 of POHA prohibits threatening, abusive, or insulting communication intended to cause harassment, alarm, or distress. Offenders under this section shall be liable to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 6 months or to both.

This provision could be applied if the creators or distributors of the deepfake pornography produced or shared the content with the intent to harm, alarm, or distress the victim. However, in most cases, harassment, alarm, or distress caused to the victim is often a byproduct of the perpetrator's primary intention of sexual gratification. Thus, the application of this provision is limited.[31]

8.2.3 Films Act 1981

Under Singapore's Films Act, the term 'film' in this Act is broadly defined to include cinematograph film or video recording, video game, or any type of recording capable of producing and displaying moving visual images. This includes images generated by computers. By including computer-generated images and any form of recordings capable of producing moving visuals, the law expanded from traditional recordings to synthetically created content such as deepfake pornography. Nevertheless, the Act regulates the possession, making, and distribution of films in general without specifically referring to content involving children.

The possession or creation of deepfake pornography may constitute an offence under Section 29 of the Films Act. This provision criminalises the making or reproducing of any obscene film, even if not for the purpose of distribution to any other person. To constitute an offence, the individual must know or have reasonable cause to believe the film is obscene.

In this Act, 'obscene' is defined as a film that has the tendency to deprave or corrupt persons who are likely to see or hear its content. Deepfake child pornography, which depicts sexually explicit material involving minors, would meet the threshold of obscenity. It is likely to have a morally corrupting influence on viewers and to bring harmful attitudes toward children.

[31] ibid.

Upon conviction under Section 29 of the Films Act, the offender may face a fine not exceeding $40,000, or to imprisonment for a term not exceeding two years, or to both.[32]

In addition, distributing or possessing any obscene films with the intent to distribute is also an offence with the penalty of a fine not exceeding $80,000 or imprisonment for a term not exceeding two years, or to both.[33] Meanwhile, merely possessing an obscene film without being the creator or the distributor also constitutes an offence under Section 30 of the Films Act, which carries a lighter penalty of fines up to $20,000 or imprisonment up to 6 months or both.

These provisions extend the legal liability beyond the initial creator of deepfake child pornography. The possessor and the distributor of deepfake child pornography can still be prosecuted under this Act.

8.2.4 Summary of Singapore's Legal Framework

To sum up, Singapore appears to hold a similar legal position to Malaysia, where both countries are lacking specific legislation to directly address the issue of deepfake pornography, particularly concerning children. Nonetheless, the Singapore Films Act can be seen as a partial solution by classifying computer-generated content as 'film'.

A Singaporean politician posted a Parliamentary question to the Minister for Home Affairs and Minister of Law of Singapore regarding:—

> 'Whether Singapore is studying South Korea's and Britain's decisions to criminalise the creation or possession of sexually explicit deepfake images and videos, and to consider these as a way to strengthen Singapore's legal regime against such forms of sexual harassment.'

The Minister clarified that their existing laws already address such concerns. The Penal Code criminalises the productions, possession, and access to such material with harsher penalties when the content involves minor. Additionally, the Minister noted that further amendments to the Penal Code are expected in 2025 to clarify that these offences apply to sexually explicit deepfakes generated though AI.[34]

8.3 South Korea

In South Korea, reports surfaced around September 2024 of police investigations into deepfake pornography rings operating at two of the country's major universities. Authorities

[32] Films Act 1981, s 29(1).

[33] Films Act 1981, s 29(3).

[34] 'Written Replies to Parliamentary Questions: Criminalisation of the Creation or Possession of Sexually Explicit Deepfake Images and Videos' (*Ministry of Home Affairs*, 5 February 2025) <https://www.mha.gov.sg/mediaroom/parliamentary/criminalisation-of-the-creation-or-possession-of-sexually-explicit-deepfake-images-and-videos/>.

discovered numerous chat groups on the messaging platform Telegram where users systematically shared photos of women they knew and used AI software to transform them into fake pornographic images within seconds. The operation was highly organised and targeted not only at university students but also at high school and middle school students. Over 500 schools and universities were identified as targets, with many victims believed to be under the age of 16. The exact number of those affected is yet to be determined.[35]

8.3.1 Act on Special Cases Concerning the Punishment of Sexual Crimes

In September 2024, South Korean lawmakers passed a revision to the Act on Special Cases Concerning the Punishment of Sexual Crimes. The amendment introduces criminal liability for individuals who purchase, possess, store, or view sexually explicit deepfake images and videos. The offenders may face imprisonment up to three years or a fine up to 30 million won.[36]

The revised law also increases the penalties for producing and distributing deepfake pornography materials by raising the maximum imprisonment sentence from five years to seven years.[37]

Furthermore, prior to the amendment, the offence for creating deepfake pornography with the purpose of distribution carried a maximum of seven years imprisonment with no minimum term. Following the revision, the law now prescribes a minimum sentence of three years with no maximum limit.[38]

The Act was also revised to strengthen protections for children and teenagers. The use of sexually exploitative material to blackmail or coerce minors is subject to harsher penalties compared to those provided under the previous law. Previously, blackmail was punishable with a minimum of one year imprisonment, whereas coercion was punishable with a minimum of three years imprisonment. The revised law now increases these penalties to a minimum of three years for blackmail and a minimum of five years for coercion.[39]

8.3.2 Sexual Violence Prevention and Victims Protection Act

The Sexual Violence Prevention and Victims Protection Act was also revised to impose a legal obligation on the government to remove the illegally filmed materials. This provision

[35] Jean Mackenzie and Leehyun Choi, 'Inside the Deepfake Porn Crisis Engulfing Korean Schools' *BBC News* (Seoul, 3 September 2024) <https://www.bbc.com/news/articles/cpdlpj9zn9go>.

[36] Yi Wonju, 'Parliamentary Committee Passes Bill Imposing Imprisonment for Possessing or Viewing Deepfake Sex Porn' *Yonhap News Agency* (Seoul, 25 September 2024) <https://en.yna.co.kr/view/AEN20240925006300315>.

[37] Lee Jung Joo, 'Cabinet Approves Bill Revision to Punish Possessing, Watching Deepfake Porn' (*The Korea Herald,* 13 November 2024) <https://www.koreaherald.com/article/3490966>.

[38] Lee Jung Joo, (n 37).

[39] Yi Wonju, (n 36).

aims to support the victims in recovering from trauma and facilitating their reintegration into normal life.

8.3.3 Summary of South Korea's Legal Framework

South Korea is among the few countries that have enacted laws specifically targeting the issue of deepfake pornography. While the legislations are not solely focused on protecting child victims, the Act on Special Cases Concerning the Punishment of Sexual Crimes includes specific provisions and punishment for perpetrators who use deepfake material to coerce or blackmail minors into engaging in more harmful activities against their will.

8.4 European Union

Aside from the national legislations adopted by the countries, European Parliament had officially approved European Union's Artificial Intelligence Act (EU AI Act) on 13 March 2024, which the Act included deepfakes technology in the discussions.

Article 3 (60) of EU AI Act defines "deepfake" as AI-generated or manipulated image, audio, or video content that resembles existing persons, objects, places, entities, or events and would falsely appear to a person to be authentic or truthful. The EU AI Act imposed transparency obligations for AI providers and deployers where deepfakes creators may fall within the scope.[40]

Article 50(1) of EU AI Act provides a general obligation on the providers where they must endure that AI system intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system.

The EU AI Act aims to address the growing concern of deepfakes and requires their creators to inform the public about the artificial nature of their work. Article 50(4) of the EU AI Act mandates the deployers of an AI system that generates or manipulates image, audio, or video content constituting a deepfake to disclose that the content has been artificially generated or manipulated. Recital 134 added on to this provision, stating that the generator of deepfakes should clearly and distinguishably disclose that the content has been artificially created or manipulated by labelling the AI output accordingly and disclosing its artificial origin.

The Commission is mandated under Article 96(1)(d) of EU AI Act to develop practical guidelines. These guidelines will specifically support the implementation of deepfake transparency obligations for providers and deployers outlined in Article 50.

[40] Felipe Romero Moreno, 'Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content' (2024) 38(3) International Review of Law, Computers and Technology 297 <https://doi.org/10.1080/13600869.2024.2324540>.

Aside from mandatory deepfake labelling and detection requirements, Article 50(7) and Recital 135 of the EU AI Act empower a two-prolonged approach led by the AI Office and Commission. Firstly, the AI Office shall facilitate the drafting of codes of practice at the Union level under Article 50(7). The codes of practice shall facilitate the effective implementation of the obligations regarding the detection and labelling of artificially generated or manipulated content. The Commission may approve the codes and implement acts as guidance, and on the other hand, may adopt stricter rules through implementing 'binding acts' if deemed the code insufficient based on a specific procedure.

Secondly, the Commission encourages the development of codes addressing broader challenges beyond just deepfakes labelling and detection. For instance, the practical arrangements for making detection mechanisms accessible, facilitating cooperation with other actors along the value chain, disseminating content, or checking its authenticity and provenance to enable the public to effectively distinguish AI-generated content.

9. Discussion

It is an unfortunate but accurate reality that the law is lagging behind the advancement of technology, particularly when it comes to the issues posed by deepfake technology.[41] In Malaysia, there is currently no specific legislation to address deepfakes created intimate content. To combat this issue, deepfakes should be regulated, monitored, and controlled through amendments to existing laws, introduction of new laws specifically targeting deepfakes, and collaboration between government, regulatory bodies and other countries.

9.1 Strengthening the Existing Legislation

First of all, existing legislation may be amended to clearly criminalise the creation, distribution, and possession of deepfakes intimate materials. For instance, under SOCA, the definition of 'child pornography' shall be expanded to include the videos or images generated using deepfake technology.

Moreover, CMA and PC should comprehensively address deepfake-related offences directly, instead of categorising deepfake intimate materials as obscene and indecent. The penalties should be made more severe, particularly when the crime is targeting vulnerable children to ensure that they serve as an effective deterrent to potential offenders.

The scope of the Content Code should be broadened to include not only industry actors but also ordinary users. This is because such technologies are now readily accessible to the general public, thus making it essential for them to be subject to the regulation as well. In addition to imposing specific obligations on ordinary Internet users, the Code should mandate the ISPs adopt stricter content moderation policies and take proactive measures to delete or report obscene or indecent content. Moreover, rather than merely suggesting that

[41] Abigail Olson, (n 20).

"deepfake pornography" is categorised as obscene or indecent content, the Code should explicitly include "deepfake pornography" in its terminology to eliminate any ambiguity.

9.2 Communications and Multimedia (Amendment) Bill 2024

In 2024, the CMA was tabled for amendment. The Communications and Multimedia (Amendment) Bill 2024 proposes significant amendments to the CMA, which include amendments to Section 211 and Section 233 of CMA.

Section 211 of CMA has been amended to cover a more restricted scope. Prior to the amendment, the provision imposed liability on both application service providers and any person using a content application service for providing indecent, false, menacing, or offensive content. However, with the amendment, the phrase 'or other person using a content applications service' will be removed.[42] Consequently, only content applications service providers can now be held accountable while users who engaged in such acts are no longer liable under this section. Nonetheless, the users of the content application service will be caught under Section 233 of CMA.

Furthermore, Section 233(3) had been amended to protect child victims. The provision states that anyone who makes, creates, or solicits and initiates the transmission of any obscene, indecent, false, menacing, or grossly offensive content directed at a child who is under the age of 18 will face a penalty of a fine up to RM500,000 or to imprisonment for a term not exceeding 5 years or to both. 'Grossly offensive' is being defined as expletive and profane in nature that offends many people, including crude references.

In addition, the definitions of obscene, indecent, false, menacing, and grossly offensive content are now included in the explanation provided under Section 233 of CMA, making them legally binding to the ISPs.

The intimate content created through deepfake technology could fall under the categories of obscene or indecent content, as discussed earlier. Additionally, it may also be considered as false content, as 'false content' is defined as content or information that is untrue, confusing, incomplete, or fabricated involving non-existing matters.

However, despite harsher penalties outlined in Section 233(1) of CMA for crimes involving children, deepfake content is still not explicitly defined or incorporated into the offences provided under CMA. Therefore, making the current provisions insufficient.

9.3 Communications and Multimedia (Licensing) (Exemption) (Amendment) Order 2024

Communications and Multimedia (Licensing) (Exemption) Order 2000 (principal Order) was amended by the Communications and Multimedia (Licensing) (Exemption) (Amendment) Order 2024, which was gazetted on 1 August 2024 and came into effect on 1 January 2025.

[42] Communications and Multimedia (Amendment) Bill 2024, s 80(b).

Order 5 of the Exemption Order exempted a list of application services from the Application Service Providers class license (ASP(C) licence) requirement. These include internet messaging services or social media services with fewer than eight million users in Malaysia. The ASP(C) license is valid for one year from the date of registration and must be renewed upon expiration, provided that the service continues to have more than eight million users in Malaysia.

The terms are defined under the Communications and Multimedia (Licensing) (Amendment) (No.2) Regulations 2024. 'Social media service' refers to an application service that uses Internet access to allow two or more users to create, upload, share, distribute, or modify content, including platforms like Facebook, Instagram, X, TikTok, and others. On the other hand, 'internet messaging service' refers to an application service that uses Internet access to allow users to communicate with one another, including platforms such as Telegram, WhatsApp, Messenger, and other similar services.

The requirement for the social media service and internet messaging service to obtain an ASP(C) licence is to ensure their compliance with regulatory obligations under the CMA, its subsidiary legislation, and any other instruments, guidelines, or regulatory policies issued under the CMA. These obligations include protecting user safety, particularly concerning online harms such as violence and child exploitation,[43] and preventing the misuse of application services to commit offences under Malaysian law.[44]

According to MCMC Deputy Managing Director Datuk Zulkarnain Mohd Yasin, the licensing measures aim to address various harms associated with technological advancements, including AI and deepfake technology.[45]

9.4 Introducing New Legislation on Deepfakes

In place of amending the existing legislation, Malaysia may take proactive measures to enact new legislation specifically aimed at tackling deepfakes. These legislations should clearly define deepfake content, such as the manipulated audio-visual materials created using artificial intelligence. The legislation should emphasise on the harmful deepfakes particularly those related to children exploitation, non-consensual pornography, and the dissemination of false information.

---

[43] APAC Region, 'New Mandatory Licensing Requirements for Application Service Providers in Malaysia' (*CMS Law-Now*, 24 January 2025) <https://cms-lawnow.com/en/ealerts/2025/01/new-mandatory-licensing-requirements-for-application-service-providers-in-malaysia?format=pdf&v=17>.

[44] 'Malaysia: Licensing of Social Media and Internet Messaging Service Providers–From 1 January 2025 Onwards' (*BakerMckenzie Insight Plus*, 5 August 2024) <https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/malaysia-licensing-of-social-media-and-internet-messaging-service-providers-from-1-january-2025-onwards#:~:text=With%20effect%20from%201%20January,1998%20(%22CMA%22)%20in>.

[45] 'MCMC Seeks Balance to Regulate Social Media Challenges' *Bernama* (Kuala Lumpur, 6 September 2024) <https://bernama.com/en/news.php?id=2337378>.

Not only by defining what is considered as deepfake content, the laws should also set out clear obligations of the ISPs, CASPs, and the regulatory bodies to implement steps to detect and prevent the spread of malicious deepfake content. For example, service providers should be required to employ AI-driven detection technologies and promptly remove harmful deepfake content to minimise harm to victims.

9.4.1 Online Safety Bill 2024

The Online Safety Bill 2024 (OSB) was passed by the Dewan Rakyat and Dewan Negara in December 2024 and is now waiting for Royal Assent before becoming law upon its being gazetted. The purpose of the Bill is to enhance and promote online safety in Malaysia by regulating harmful content and establishing obligations of application service providers, content application service providers, and network service providers. The Malaysian Communications and Multimedia Commission (MCMC) will enforce the Bill to reduce harmful content online and mitigate its potential negative impacts.

The Bill mandates social media platform providers to fulfil three primary duties, namely ensuring platform safety, protecting children under the age of 13, and restricting access to harmful content.[46] The recently tabled Bill includes provisions that specifically aim to protect children from online exploitation.

Besides, according to Section 4 of OSB, the Bill will have extraterritorial effect and will apply to individuals outside Malaysia who are licensed under the CMA and who provide any application service, content application service, or network service within Malaysia.

The First Schedule of the Bill outlines the types of content classified as 'harmful content' with one of them including child sexual abuse material as defined under Section 4 of SOCA. This content is categorised as "priority harmful content" and is subject to stricter regulations compared to other cybercrimes.[47]

Another important aspect of the Bill is the establishment of the 'Online Safety Committee' under Section 5 of OSB. The Committee will include a Chairman and Deputy Chairman, along with representatives from various Ministries such as communications, home affairs, digital-related matters, education, and women, family, and community development. Each of the licensed applications service providers, licensed content applications service providers, and licensed network service providers will also appoint a representative to be part of the Committee. The Committee's role is to advise and give recommendations to the MCMC on online safety matters, including the determination of priority harmful content.

---

[46] Bernama, 'Online Safety Bill to Mandate Three Key Responsibilities for Platform Providers' *Awani International* (Kuala Lumpur, 16 October 2024) <https://international.astroawani.com/malaysia-news/online-safety-bill-mandate-three-key-responsibilities-platform-providers-491978>.

[47] 'Online Safety Bill 2024 Passed by Malaysian Parliament' (*Skrine*, 17 December 2024) <https://www.skrine.com/insights/alerts/december-2024/online-safety-bill-2024-passed-by-malaysian-parlia>.

Furthermore, OSB also stated the duties of licensed application service providers and licensed content application service providers under Part III of the Bill. Among other obligations, they are required to implement measures to mitigate the risk of exposure to harmful content, make available mechanism for reporting harmful content, establish a mechanism for making priority harmful content inaccessible and so on.

This Bill could potentially serve as new legislation to curb the spread of exploitative deepfake content online by imposing stricter obligations on service providers. Notwithstanding, it remains insufficient in addressing the issue of deepfake intimate materials leading to child exploitation, as the legislation is not specifically tailored to tackle this problem.

Both approaches, namely amending existing laws or enacting new legislation to address deepfake child pornography, should be carefully considered. However, it is suggested that introducing a standalone legislation would be more practical as deepfake technology is an emerging and complex field that demands detailed and specific regulation. Currently, relevant laws are scattered across various statutes. Therefore, even if existing laws are amended to cover deepfake pornography, it may still pose challenges for law enforcement, prosecutors, and the judiciary to cross-reference and apply multiple legal regulations effectively. A comprehensive and standalone law would provide greater clarity and consistency.

9.4.2 Enhancing Collaboration

Aside from amending and enacting legislations, Malaysia's government should also take steps to collaborate with other bodies and countries for better enforcement of the legislations and to facilitate cross-border investigations, information sharing, and joint operations in tackling deepfake-related crimes more effectively.

Within Malaysia, the government should form or empower existing sectoral regulators or enforcement bodies to augment capabilities and regulate activity that is now AI-enabled, such as the creation and alteration of videos through deepfakes technology.[48] In Malaysia, the responsibility in monitoring, regulating, and taking actions against deepfake content would fall on MCMC. Therefore, MCMC, as the primary regulatory body, shall be empowered with greater enforcement power to monitor and even enact necessary commissions or codes against the deepfakes content.

International cooperation and harmonisation of laws across jurisdictions could enhance the ability to combat cross-border online crimes[49] in the way of collecting and using digital evidence, as cybercrime is a global crime. The deepfakes content is created often across borders. The state shall join international agreements and conventions to ensure the support

[48] Farlina Said and Farah Nabilah, 'Future of Malaysia's AI governance' (Institute of Strategic & International Studies Malaysia 2024) <https://www.isis.org.my/wp-content/uploads/2024/12/AI-Governance-white-paper.pdf>.

[49] 'Deepfakes and Online Scams' (n 22).

from other states.[50] Enabling cross-border investigations and joint enforcement actions between the nations will ensure that the perpetrators cannot evade accountability by exploiting jurisdictional gaps.

10. Conclusion

In conclusion, deepfake technology presents profound risks especially concerning child exploitation. The existing legal frameworks in Malaysia demonstrate significant loopholes in addressing the challenges posed by this technology. Comparative analysis reveals that while countries like the UK, South Korea, and regions such as European Union have taken steps to regulate deepfake-related crime, Malaysia's approach remains fragmented and insufficient.

Ultimately, banning deepfakes technology would stifle its legitimate and creative uses, especially in the film industry. However, allowing it to go unregulated would lead to a world filled with uncertainties and mistrust. Thus, it is the responsibility of international organisations and national institutions to establish specific legislation to ensure that the deepfake contents are properly controlled and its use is closely monitored.

Hence, Malaysia may reform the existing legislation or enact a new law to explicitly criminalise deepfake technology. The enactment of specific laws targeting deepfake technology and its misuse, coupled with stricter penalties for crimes involving children, is necessary to provide them a better protection. For instance, Malaysia's legal framework should define the words 'film' or 'image' by including the photograph or images created by computer graphics or digital technologies similar to the UK's Criminal Justice Bill or Online Safety Act. Meanwhile, the deepfake pornography related crimes should not be restricted to the creation, distribution, and possession of such content. Malaysia's law should also criminalise the malicious use of deepfake pornography, such as to cause distress, harm, and to threaten victims, as outlined in the legal framework of the UK and South Korea.

Furthermore, collaborative efforts with international bodies and cross-border cooperation through conventions and treaties will be helpful in addressing the global nature of deepfake crimes. Striking a balance between innovation and safeguarding societal values is essential to ensure that advancements in AI serve the greater good without enabling exploitation.

Acknowledgement

I would like to express my sincere gratitude to everyone who contributed to the completion of this research paper.

First and foremost, I extend my deepest appreciation to my supervisor, Dr Manique Cooray, for her invaluable guidance, constructive feedback, and unwavering support

[50] Mohamed Hassan Mekkawi (n 21).

throughout this research journey. Her expertise and advice have been instrumental in shaping this paper.

I would also like to acknowledge Multimedia University for providing necessary resources and a conducive environment for my research, including academic databases and libraries have been invaluable in the development of this paper.

Lastly, my heartfelt appreciation goes to my family and friends for their continuous support and encouragement have been my source of strength throughout this process.

Funding Information

The authors received no funding from any party for the research and publication of this article. ◆