# IMPLICATIONS OF AI ON CYBERCRIME AND THE LEGAL GAPS

***Lim Yi Ern***[1*]

**Abstract**

Artificial Intelligence has become increasingly embedded in key sectors across Malaysia, bringing advancements in efficiency, personalization, and data analysis. However, its integration into digital systems has also led to new and complex forms of cybercrime. Technologies such as DeepFake, AI-generated phishing, and more are being exploited in ways that challenge conventional legal definitions and enforcement mechanisms. Malaysia's current legal framework, including existing cyber laws, lacks the specificity and scope to adequately address these evolving threats. This article seeks to explore the emerging risks posed by AI-driven cybercrimes and critically examines the limitations of Malaysia's present legal provisions. Through the analysis of legal documents and reference to recent case studies and expert commentaries, this article seeks to highlight how current laws fall short in regulating AI misuse. It underscores the urgency of adapting legal systems to the technological realities of AI in order to safeguard individuals, institutions, and the integrity of Malaysia's digital landscape.

## 1.0 Introduction

The rapid growth of cybercrime in recent years has been recognised as a shared global concern.[2] Malaysia is no exception, with cases rising sharply year after year.[3] For instance, according to the Department of Statistics Malaysia (DOSM), online crime cases surged by 35.4% in 2023

[1*] LLB (Honours) candidate under the HULLB programme, HELP University.

[2] 'Safeguarding Malaysia from Cyberthreats' (*Netsweeper*, 21 May 2025) <https://www.netsweeper.com/government/safeguarding-malaysia-from-cyberthreats> accessed 15 August 2025.

[3] Khairul Akma Mahamad & Raja Nur Zafira Raja Sharudin, 'CYBERCRIMES: TYPES & TIPS' (*THOUGHTS*, 13 December 2023) <https://www.bernama.com/en/thoughts/news.php?id=2253495> accessed 15 August 2025.

compared to 2022, rising from 25,479 to 34,532.[4] While cybercrime is a complex issue on its own, the emergence of Artificial Intelligence (hereinafter referred to as the 'AI') has added new layers of complexity, as it not only defends against cybercrime but also escalates it.[5]

The primary purpose of this article is to examine how AI is transforming the landscape of cybercrimes, both positively and negatively, and to identify the legal loopholes in Malaysia's current cyber laws. It will begin with an introduction to cybercrime, which includes the definition and common types, and followed by a brief overview of AI. The discussion will then analyse how AI is used to combat cybercrime and how cybercriminals exploit it to carry out attacks, before finally assessing the current laws and their gaps.

## 2.0 What is Cybercrime?

According to the Cambridge Dictionary, 'cyber' refers to anything involving, using or relating to computers; while 'crime' denotes unlawful activities. Thus, the word "cybercrime" means any criminal conduct that involves the use of a computer or a networked device, as a tool to target the victim.[6] Unlike physical crimes, cybercrime can easily cross borders within a short span of time.[7]

More often than not, the primary motive behind cybercrime is financial gain.[8] This is demonstrated by the fact that in 2024, online scams caused staggering losses of RM1.5 billion, amounting to 35,368 reported cases.[9] There are also those who commit cybercrimes for other reasons, such as harming personal integrity or valuable information.[10]

---

[4] 'Online crime cases rose by 35.5% in 2023, says DOSM' *The Malaysian Reserve* (16 October 2024) <https://themalaysianreserve.com/2024/10/16/online-crime-cases-rose-by-35-5-in-2023-says-dosm/ > accessed 16 August 2025.

[5] Najihah Borhan, 'Alarming rise in AI-driven cybercrimes reported this year, says CCID chief' *New Straits Times* (20 January 2025) <https://www.nst.com.my/news/nation/2025/01/1163648/alarming-rise-ai-driven-cybercrimes-reported-year-says-ccid-chief> accessed 15 August 2025.

[6] Joseph Aghatise, 'Cybercrime Definition' (*Research Gate*, June 2006) <https://www.researchgate.net/publication/265350281_Cybercrime_definition> accessed 16 August 2025.

[7] Ahmad Redzuan Mohamad, Mohd Rizal Yaakop and Mohd Azmi Mohd Razif, 'The Efficacy of the Malaysian Government's Response towards Cybercrime' Open Journal of Political Science*, 14, 166-176*. <https://doi.org/10.4236/ojps.2024.141010> accessed 17 August 2025.

[8] 'What is cybercrime? How to protect yoursel' (*Kaspersky*, -) <https://www.kaspersky.com/resource-center/threats/what-is-cybercrime> accessed 16 August 2025.

[9] Qistina Sallehuddin, 'Cybercrime losses exceed RM1.5bil in 2024' *New Straits Times* (18 February 2025) <https://www.nst.com.my/news/nation/2025/02/1176474/cybercrime-losses-exceed-rm15bil-2024> accessed 17 August 2025.

[10] Sitti Syamsiar Muharam, Mohd Zuhairizan Suhaimi and Markrandy Marcus, '34 CYBERCRIMES IN MALAYSIA' (*Research Gate*, February 2023) <https://www.researchgate.net/publication/367655136_CYBERCRIMES_IN_MALAYSIA> accessed 20 August 2025.

## 3.0 Types of Cybercrimes

Cybercrimes can take many forms, including phishing, ransomware, identity theft, hacking, cyberbullying or harassment and cyber child pornography. For the purpose of this article, the discussion will focus on phishing, malware, cyberbullying and cyber child pornography.

### 3.1 Phishing

Generally, phishing is a cybercrime in which criminals impersonate legitimate entities, such as banks, e-commerce platforms or government agencies, to deceive individuals into revealing sensitive information like credit card details or online banking credentials through emails, messages and fraudulent websites.[11] For example, the Chief Executive Officer (CEO) of Cyber Security Malaysia (CSM), Datuk Dr. Amirudin Abdul Wahab, highlighted cases where subscription services such as Spotify and Netflix were spoofed to obtain users' payment details.[12] This type of phishing is typically aimed at financial theft, or in some cases, identity theft, as attackers may either seek for payment details or personal information, or both.[13]

Another well-known form of phishing is spear-phishing, where a specific individual or organisation is deliberately targeted, often to compromise the organisation's security through the spread of malware.[14] In such cases, the recipient may receive an email appearing to come from someone they know, such as a manager or colleague, to build trust. Once the victim clicks on the malicious link or attachment, malware is executed, and not only does it threaten the individual's device but also the entire network to which the device is connected to.[15] Unlike traditional phishing, which relies on generic mass emails, spear-phishing is highly personalised to exploit trust and maximise its impact.[16]

---

[11] Shauqi Wahab & Hidayath Hisham, 'The mounting landscape of phishing scams in Malaysia' *The Malaysian Reserve* (23 January 2025) <https://themalaysianreserve.com/2025/01/23/the-mounting-landscape-of-phishing-scams-in-malaysia/> accessed 17 August 2025.

[12] *Ibid*.

[13] Ahmad Redzuan Mohamad, Mohd Rizal Yaakop and Mohd Azmi Mohd Razif, 'The Efficacy of the Malaysian Government's Response towards Cybercrime' 14 Open Journal of Political Science, 166-176 <https://doi.org/10.4236/ojps.2024.141010> accessed 17 August 2025.

[14] *Ibid*.

[15] Aleeya Fatinah Ahmad Fauzey and Associate Professor Dr. Manique Cooray, 'Examining the Legal Responsibilities of Spear Phishing Attacks in Malaysia' (ICLD 2023), Advances in Social Science, Education and Humanities Research <https://doi.org/10.2991/978-2-38476-154-8_6> accessed 17 August 2025.

[16] Douglas C Youvan, 'Spear-Phishing: A Deep Dive into the Art of Targeted Cyber Deception' (*Research Gate*, 20 October 2024) <https://www.researchgate.net/publication/385105403_Spear-Phishing_A_Deep_Dive_into_the_Art_of_Targeted_Cyber_Deception > accessed 18 August 2025.

### 3.2 Malware

Malware occurs when code in a software system is added, altered, or removed with an intent to harm or disrupt the system's intended function.[17] In simple terms, a computer network becomes infected with a virus. Malware can cause significant loss of information and money, and in some cases, even threaten lives, as it has the potential to compromise medical devices.[18]

Ransomware is a type of malware in which criminals encrypt files on victims' servers, and then demand a ransom from victims, mostly in cryptocurrency, to unlock the files.[19] It is usually spread through phishing emails or by tricking users into downloading malicious files. It poses a serious threat to organisations, as it can cause financial losses, reputational damage, and even operational shutdowns.[20] The severity of ransomware can be seen in the global WannaCry attack in 2017, which affected approximately 230,000 computers across 150 countries and caused an estimated $4 billion in financial losses.[21] The threat is equally pressing in Malaysia, where many companies have suffered ransomware attacks, with cases rising up to 78% in the fourth quarter of 2024 compared to the previous quarter.[22]

### 3.3 Cyberbullying

According to the United Nations International Children's Emergency Fund (UNICEF), cyberbullying refers to bullying that occurs through digital technologies, typically via social

[17] Anitta Patience Namanya, Andrea J. Cullen, Irfan Awan and Jules Pagna Diss, 'The World of Malware: An Overview' (*Research Gate*, September 2018) <https://www.researchgate.net/publication/327665678_The_World_of_Malware_An_Overview> accessed 18 August 2025.

[18] Richard G. Brody, Harold U. Chang and Erich S. Schoenberg, 'Malware at its worst: death and destruction' 26(4) IJAIM <https://doi.org/10.1108/IJAIM-04-2018-0046> accessed 18 August 2025.

[19] Muhammad Ubale Kiru and Jantan Aman 'The Age of Ransomware: Understanding Ransomware and Its Countermeasures.' (2019) IGI Global <https://doi.org/10.4018/978-1-5225-7353-1.ch001> accessed 18 August 2025.

[20] Mohamed Marjook Hussain, 'Toolkit: Staying ahead: How to avoid being a victim of ransomware' *The Edge Malaysia* (11 August 2025) <https://theedgemalaysia.com/node/765880> accessed 19 August 2025.

[21] 'What is cybercrime? How to protect yourself' (*Kaspersky*) <https://www.kaspersky.com/resource-center/threats/what-is-cybercrime> accessed 16 August 2025.

[22] Mohamed Marjook Hussain, 'Toolkit: Staying ahead: How to avoid being a victim of ransomware' *The Edge Malaysia* (11 August 2025) <https://theedgemalaysia.com/node/765880> accessed 19 August 2025.

media, gaming and messaging platforms, and mobile phones.[23] People engage in cyberbullying for various reasons, such as amusement, revenge, jealousy, or simply to seek attention.[24]

According to Statista, internet users may be exposed to cyberbullying, with teenagers representing a particularly high-risk demographic.[25] Common forms of cyberbullying include posting malicious comments online, circulating rumours about an individual, making racial or sexist remarks, sharing hurtful images, and issuing threats via calls or text messages.[26] Notably, cyberbullying can have serious and adverse impacts on mental health, including diminished self-esteem, emotional distress, and, in extreme cases, suicidal tendencies.[27]

### 3.4 Cyber Child Pornography

Child pornography is defined as the 'sexual exploitation and abuse of children in pornographic materials and performances'.[28] Children depicted in such materials are subjected to extreme and brutal sexual acts. This has long been criminalised in Malaysia, where it is classified as child sexual abuse material rather than child porn,[29] governed under the **Sexual Offences against Children Act 2017**.[30] With the transformation and proliferation of technologies, including the internet and mobile devices, this crime has become increasingly widespread and transcends geographical boundaries, facilitated through online connectivity such as live streaming platforms

[23] Nurulhuda Ahmad Razali, Nazli Ismail Nawang and S.N.A. Syed Nong, 'CYBERBULLYING IN MALAYSIA: AN ANALYSIS OF THE EXISTING LAWS' (*Research Gate*, 28 December 2022) <https://www.researchgate.net/publication/367198006_CYBERBULLYING_IN_MALAYSIA_AN_ANALYSIS_OF_THE_EXISTING_LAWS> accessed 19 August 2025.

[24] Sitti Syamsiar Muharam, Mohd Zuhairizan Suhaimi and Markrandy Marcus, '34 CYBERCRIMES IN MALAYSIA' *Research Gate* (February 2023) <https://www.researchgate.net/publication/367655136_CYBERCRIMES_IN_MALAYSIA> accessed 20 August 2025.

[25] Stacy Jo Dixon, 'Cyberbullying - statistics & facts' (*statista*, 24 October 2024) <https://www.statista.com/topics/1809/cyber-bullying/#topicOverview> accessed 19 August 2025.

[26] Azriq Ariffin, Nurul Mohd, and Thurgeaswary Rokanatnam, 'Cyberbullying via Social Media: Case Studies in Malaysia' (2021) 3(1) OIC-CERT Journal of Cyber Security <https://www.oic-cert.org/en/journal/pdf/3/1/313.pdf> accessed 19 August 2025.

[27] *Ibid*.

[28] Kirama Nasim Manbi Ushama, & Juriah binti Abdul Jalil, 'MALAYSIA'S LEGAL RESPONSE TO TACKLING THE CRIME OF ONLINE CHILD PORNOGRAPHY' 28(1) IIUM Law Journal, 165–195 <https://doi.org/10.31436/iiumlj.v28i1.449> accessed 21 August 2025.

[29] 'New report finds promising government initiatives to help end online child sexual exploitation and abuse in Malaysia' *Unicef Malaysia* (21 September 2022) <https://www.unicef.org/malaysia/press-releases/report-finds-promising-government-initiatives-help-end-online > accessed 26 August 2025.

[30] Ida Lim, 'Make no mistake, downloading and viewing 'child porn' is a crime in Malaysia — here's what the numbers tell us' *Malay Mail* (8 January 2024) <https://www.malaymail.com/news/malaysia/2024/01/08/make-no-mistake-downloading-and-viewing-child-porn-is-a-crime-in-malaysia-heres-what-the-numbers-tell-us/108340> accessed 21 August 2025.

and cloud storage.[31] In fact, it has become a multibillion-dollar industry, with offenders constantly being active in cyberspace, leaving minors to suffer re-victimisation each time these images or videos are viewed, as the content remains permanently accessible.[32]

## 4.0 Reshaping of Cybercrime by AI

Before examining how AI has reshaped the landscape of cybercrime, it is crucial to first understand what AI encompasses.

### 4.1 Introduction to AI

AI refers to the technology that allows computers and machines to perform tasks that typically require human intelligence,[33] ranging from pattern recognition[34] to learning, decision-making, problem-solving, creativity and even acting autonomously.[35] These capabilities are enabled through the fundamental components of AI:

1) Machine Learning (ML): A subset of AI that equips systems with the ability to improve performance autonomously through continuous exposure to data.

2) Deep Learning (DL): A subset of Machine Learning (ML) that analyses complex patterns within large-scale data. DL has been the cornerstone in advancements of autonomous driving, image and voice recognition, and Natural Language Processing (NLP).

3) Natural Language Processing (NLP): A field that allows AI to comprehend, interpret, and generate human language. Applications include language translation systems, chatbots and voice assistants.

4) Computer Vision: Enables AI systems to interpret visual information, with applications ranging from facial recognition to medical imaging analysis.

---

[31] Kirama Nasim Manbi Ushama, & Juriah binti Abdul Jalil, 'Malaysia's Legal Response To Tackling The Crime Of Online Child Pornography' 28(1) IIUM Law Journal, 165–195 <https://doi.org/10.31436/iiumlj.v28i1.449> accessed 21 August 2025.
[32] 'Child Sexual Abuse Material' *National Center for Missing & Exploited Children* <https://www.missingkids.org/theissues/csam> accessed 21 August 2025.
[33] Cole Stryker and Eda Kavlakoglu, ' What is artificial intelligence (AI)?' (*IBM*, 9 August 2024) <https://www.ibm.com/think/topics/artificial-intelligence> accessed 22 August 2025.
[34] Dhruvitkumar Talati, Blessing Joe and George Smart, 'AI (Artificial Intelligence) in Daily Life' (*ResearchGate*, 9 May 2024) <https://www.researchgate.net/publication/380434525_AI_Artificial_Intelligence_in_Daily_Life > accessed 2 August 2025.
[35] *Ibid*.

Each component operates through algorithms that analyse data, recognise patterns and generate inferences.

### 4.2 AI Application in Daily Life

The evolution of AI has led to virtual integration in every aspect of human life.[36] AI is leveraged not only across industries such as healthcare, finance, education, and manufacturing, but also in routine daily activities. Below are some common examples of AI applications in everyday life.

1) Communication:

   The AI system employing Natural Language Processing (NLP) allows voice assistants such as Apple's Siri or Google Assistant to comprehend and respond to voice commands, providing users with convenient control over smart devices and search functions.[37] Moreover, AI chatbots, which are available 24/7, ensure prompt and efficient responses to customer queries.

2) Healthcare:

   AI has significant applications in the healthcare sector. For instance, its data analysis capabilities allow AI systems to predict the health outcomes of a patient from medical records and identify subtle patterns in medical images, such as CT scans and X-rays, that may not be discernible to the human eye.[38]

3) Education:

   AI-based learning platforms, such as 360Learning and Absorb LMS, provides personalised and adaptive content tailored to students' performance, thereby enhancing their learning outcomes.[39] In addition, AI can deliver real-time feedback, allowing

[36] Darrell M. West and John R. Allen, 'How artificial intelligence is transforming the world' (*Brookings*, 24 April 2018) <https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/> accessed 8 August 2025.
[37] Dhruvitkumar Talati, Blessing Joe and George Smart (n 33).
[38] 'Artificial Intelligence in healthcare' (*europa.eu*) <https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en> accessed 20 August 2025.
[39] Amit Das and Sanjeev Malaviya, 'AI-Enabled Online Adaptive Learning Platform and Learner's Performance: A Review of Literature' (2024) 23(Special Issue 3) Empirical Economics Letters <https://doi.org/10.5281/zenodo.14002543> accessed 26 August 2026.

students to receive immediate guidance and support.[40] Such applications demonstrate the positive contributions of AI to education.

4) Social Media:

   By analysing user interactions, AI can deliver personalised content. Social media algorithms use data on user preferences to make accurate content recommendations, enabling the creation of a tailored feed for each individual user.[41]

5) Security and Surveillance:

   Many modern security cameras incorporate AI features such as facial recognition and motion detection. These capabilities enable systems to identify familiar faces, detect unusual activities, and track movements, thereby providing a higher level of protection. In addition, AI-powered security systems can send real-time alerts to homeowners when specific events occur, such as a window breaking or an unauthorized entry, via smartphone applications, allowing users to respond promptly from any location.[42]

To summarise, the advancements and convenience brought by AI shows its pervasive presence in our lives. It simplifies tasks, boosts productivity, and delivers personalised experiences, ultimately making life more convenient and efficient.[43]

### 4.3 A Double-Edged Sword in Cybercrime

In the realm of cybercrime, AI has emerged as a double-edged sword. On one end, it provides powerful tools that assist in preventing, detecting, and investigating cyberattacks.[44] On the other hand, the same technology is being weaponised by criminals to execute increasingly

[40] *Ibid*.
[41] Birkan Koç, 'The Role Of User Interactions In Social Media On Recommendation Algorithms: Evaluation Of Tiktok's Personalization Practices From User's Perspective' (2023) <https://www.researchgate.net/publication/375775130_The_Role_of_User_Interactions_in_Social_Media_on_Recommendation_Algorithms_Evaluation_of_TikTok's_Personalization_Practices_From_User's_Perspective> accessed 26 August 2026.
[42] Dhruvitkumar Talati, Blessing Joe and George Smart (n 33).
[43] *Ibid*.
[44] Anis Zalani, 'Gobind: Digital Ministry developing AI tool to detect deepfakes, fight cybercrime' *Malay Mail* (5 August 2025) <https://www.malaymail.com/news/malaysia/2025/08/05/gobind-digital-ministry-developing-ai-tool-to-detect-deepfakes-fight-cybercrime/186538 > accessed 16 August 2025.

sophisticated and large-scale attacks.[45] This section will first examine how AI contributes positively to the fight against cybercrime, before turning to the threats and challenges it poses when exploited by malicious actors.

### 4.3.1 AI: A New Shield Against Cybercrime

Today, cybersecurity is increasingly strengthened by AI technologies, particularly Machine Learning (ML) algorithms,[46] which perform functions such as automated threat detection, large-scale data analysis, and automated incident response. These applications will be discussed below.

**Advanced Threat Detection**

To begin with, AI-powered cybersecurity tools enhance threat detection. Firstly, it analyses data and learns typical patterns within a network.[47] Subsequently, it identifies unusual interactions by indicating the possible threats. Additionally, exceptionally hard-to-detect threats, such as lateral movement— a tactic used by cybercriminals to navigate networks undetected— can also be detected using AI combined with machine learning. With large-scale and real-time data analysis, these tools perform threat detection with unprecedented speed and accuracy compared to traditional methods.[48]

**Spontaneous Responses to Threats**

Moreover, AI tools can respond automatically to detected threats.[49] For example, preset actions, usually through isolating impacted devices, blocking harmful network traffic or alerting security

[45] Blake Hall, 'How AI-driven fraud challenges the global economy – and ways to combat it' (*World Economic Forum*, 16 January 2025) <https://www.weforum.org/stories/2025/01/how-ai-driven-fraud-challenges-the-global-economy-and-ways-to-combat-it/> accessed 15 May 2025.
[46] Christine Ferrusi Ross, 'AI in Cybersecurity: How AI Is Impacting the Fight Against Cybercrime' (*Akamai*, 25 May 2025) <https://www.akamai.com/blog/security/ai-cybersecurity-how-impacting-fight-against-cybercrime> accessed 16 August 2025.
[47] *Ibid*.
[48] Nidhi Nigam, 'The Role of Artificial Intelligence and Machine Learning in Enhancing Cybersecurity against Cybercrime' (*Cybersecurity Exchange*, 30 November 2024) <https://www.eccouncil.org/cybersecurity-exchange/network-security/role-of-ai-ml-in-enhancing-cybersecurity-against-threats/> accessed 23 August 2025.
[49] Christine Ferrusi Ross (n 45).

teams, will be executed to eliminate the risk. Furthermore, instead of responding randomly, these systems evaluate threat severity and allocate responses by priority. Similar to threat detection, AI-automated incident response reduces risks and potential damage far more efficiently than conventional methods, as it can handle multiple threats concurrently.

**Threat Prediction Intelligence**

By analysing historical trends, AI can anticipate and counter cyber threats.[50] This process involves examining past incident reports, security logs, and other relevant data which enables cybersecurity agencies to deepen their understanding of typical cyber threats. As a result, these systems can predict potential future threats and proactively implement preventative measures.

**Verifying Content Authenticity**

In early August 2025, Malaysia's Minister of Digital revealed the Ministry is working on an AI system designed to aid cybercrime investigations, particularly in cases of identity theft, online scam, and dissemination of false content.[51] Its main function is to authenticate images and videos.

Indeed, one of the key reasons AI is deployed in combating cybercrime lies in its ability to analyse, recognise and verify the authenticity of digital content. For example, AI tools can scan a document's attributes, such as text, fonts, layout, and images, thereby flagging suspicious elements that deviate from expected patterns.[52] Likewise, forgery detection becomes more efficient as AI algorithms can compare a signature against a verified sample stored in a shared database by assessing unique features like stroke patterns and pressure points.[53] In essence, AI enables the verification of tampering that may not be visible to the human eye.

[50] *Ibid*.
[51] 'Govt developing AI guidelines to combat online scams, to be ready early 2026' *The Star* (5 August 2025) <https://www.thestar.com.my/news/nation/2025/08/05/govt-developing-ai-guidelines-to-combat-online-scam-to-be-ready-early-2026> accessed 19 August 2025.
[52] 'The Role of Artificial Intelligence in Document Authentication' (*Innov8tive Solutions*, 18 August 2023) <https://innov8tif.com/the-role-of-artificial-intelligence-in-document-authentication/ > accessed 20 August 2025.
[53] *Ibid*.

### 4.3.2 AI: A New Weapon in Cybercrime

Undeniably, AI plays a pivotal role in bolstering cybersecurity. It has simultaneously escalated cybercrime, sparking widespread alarm among individuals and institutions alike. As highlighted by the Director of Malaysia's Commercial Crime Investigation Department, the increasing use of AI in cybercrime is among the most concerning developments in recent years.[54] This concern is substantiated by a 2025 study conducted by the International Data Corporation (IDC), which revealed that 54 percent of organisations in Malaysia experienced a twofold increase in AI-driven cyber threats, while 24 percent reported a tripling in such attacks.[55] In light of this, the following section will explore how AI is driving the transformation of cybercrime in this era.

**Errorless and More Convincing Scams**

Previously, phishing attacks launched through emails, malicious websites, or messages were relatively easy to detect,[56] as they often contained clerical errors, inaccurate details such as names or email addresses, and poor formatting.[57] However, AI has effectively addressed these shortcomings, increasing the sophistication of phishing attacks through its advanced algorithms.

The common indicators of traditional phishing attacks have been eliminated through the use of generative AI tools, such as the widely known ChatGPT, which are now readily at the fingertips of cybercriminals.[58] Even if the creator of a phishing attempt does not speak the target language, AI-generated content can produce communications that appear flawless, polished, and highly convincing to victims, making them far more difficult to detect.

---

[54] Najihah Borhan, 'Alarming rise in AI-driven cybercrimes reported this year, says CCID chief' *New Strait Times* (20 January 2025) <https://www.nst.com.my/news/nation/2025/01/1163648/alarming-rise-ai-driven-cybercrimes-reported-year-says-ccid-chief> accessed 13 August 2025.

[55] 'AI-Driven cyber threats surge in Malaysia, Fortinet warns' *The Vibes.com* (29 May 2025) <https://www.thevibes.com/articles/news/108778/ai-driven-cyber-threats-surge-in-malaysia-fortinet-warns> accessed 21 August 2025.

[56] Leah Sodoian, 'AI-Powered Cybercrime: Is Your Business Ready to Defend?' *UpGuard* (26 June 2025) <https://www.upguard.com/blog/ai-cybercrime > accessed 11 August 2025.

[57] Sharon Shea and Ashwin Krishnan, 'How AI is making phishing attacks more dangerous' *Tech Target* (22 October 2024) <https://www.techtarget.com/searchsecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous> accessed 22 August 2025.

[58] Ashley D'Andrea, 'How AI Is Making Phishing Attacks More Dangerous' *Keeper* (13 September 2024) <https://www.keepersecurity.com/blog/2024/09/13/how-ai-is-making-phishing-attacks-more-dangerous/ > accessed 20 August 2025.

In addition, AI can craft tailored and personalised content that makes phishing attempts appear more realistic and convincing, as it can learn patterns from the data it analyses. For example, AI's Large Language Models (LLMs) can process real-time information from sources such as social media, email structures, news outlets or company websites, allowing them to incorporate up-to-date content into phishing emails.[59] As a result, victims are more likely to perceive the emails as genuine and fall for the scam.

This was demonstrated in an experiment conducted by Singapore's Government Technology Agency and presented at Black Hat USA 2021.[60] In this study, a group of users received simulated spear-phishing emails from the security team, some of which were human-crafted while others were produced by OpenAI's GPT-3. The results revealed that a greater number of users clicked on links contained in the AI-generated emails compared to those written by humans.

**Larger-Scale Attacks at Faster Rates**

AI automation enables cybercriminals to conduct attacks faster and at a larger scale. For example, AI-driven ransomware can autonomously scan security systems of targeted networks or servers to identify vulnerabilities, and then deploy the most effective tools to exploit them.[61] This allows cybercriminals to operate at much higher speed and reach far more targets without relying on human operators. Furthermore, after processing data in documents and files using Natural Language Processing (NLP), AI can automatically prioritise targets based on their priority and sensitivity. Then, it executes the ransomware attack against the most sensitive data in a predetermined sequence.

**Deepfake Technology**

[59] Sharon Shea and Ashwin Krishnan (n 56).
[60] Eugene Lim, Glenice Tan, Tan Kee Hock and Timothy Lee, 'Turing in a Box: Applying Artificial Intelligence as a Service to Targeted Phishing and Defending against AI-generated Attacks' (*GovTech Singapore*) <https://i.blackhat.com/USA21/Wednesday-Handouts/US-21-Lim-Turing-in-a-Box-wp.pdf> accessed 23 August 2025.
[61] Christine Ferrusi Ross (n 45).

With Deepfake technology, AI can now replicate a person's voice and facial features to deceive victims.[62] This process, often referred to as voice cloning and facial re-enactment, was highlighted by CyberSecurity Malaysia (CSM) CEO, Datuk Dr. Amirudin Abdul Wahab.[63] At its core, Deepfake relies on two key algorithms: the generator, which uses sample images, audio, or video to create new media, and the discriminator, which evaluates distinctive traits within the samples and guides the generator to correct anomalies.[64]

As expected, the misuse of this technology has fueled a rise in cybercrime cases, including phishing attacks and fraudulent investment scams. In 2024, a travel agent in Kuala Terengganu lost RM49,800 after receiving a call that perfectly mimicked her friend's voice, convincing her to transfer money. Similarly, fabricated videos of Prime Minister Datuk Seri Anwar Ibrahim and business tycoon Tan Sri Robert Kuok endorsing fake investment schemes circulated widely online. Such manipulations pose a serious challenge, as they are often indistinguishable from genuine content, seamlessly inserting individuals into photos or videos in which they never actually appeared.[65]

## 5.0 Cyber Laws and the Gaps

As of today, Malaysia has no legislation that specifically governs the use or misuse of AI.[66] In May 2025, the Minister of Science, Technology and Innovation Ministry (MOSTI), Chang Lih Kang, confirmed that there are currently no plans to introduce dedicated laws to regulate AI-related issues.[67] Consequently, the existing cyber laws remain the primary legal recourse for addressing cybercrimes in the country, even when AI is involved. However, these laws are not without their shortcomings. This article will thus examine the limitations within the current legal

---

[62] Sally Adee, 'What Are Deepfakes and How Are They Created?' (*IEEE Spectrum*, 29 April 2020) < https://spectrum.ieee.org/what-is-deepfake> accessed 24 August 2025.

[63] 'Can you distinguish between reality and deepfake?' *Awani International* (23 February 2025) <https://international.astroawani.com/malaysia-news/can-you-distinguish-between-reality-and-deepfake-509400> accessed 25 August 2025.

[64] 'Deepfake: How the Technology Works & How to Prevent Fraud' (*Unit 21*) <https://www.unit21.ai/fraud-aml-dictionary/deepfake> accessed 25 August 2025.

[65] Sally Adee, 'What Are Deepfakes and How Are They Created? Deepfake technologies: What they are, what they do, and how they're made' (*IEEE.ORG*, 29 April 2020) <https://spectrum.ieee.org/what-is-deepfake> accessed 3 June 2025.

[66] Vanessa Gomes, 'Cybersecurity: AI use by cybercriminals on the rise' *THE EDGE* (23 October 2025) <https://theedgemalaysia.com/node/687039> accessed 1 June 2025.

[67] Heirul Kamel, 'MOSTI: No Plans For AI Law In Malaysia Yet' (*lowyat.net*, 5 May 2025) <https://www.lowyat.net/2025/350457/mosti-no-plans-for-ai-law-in-malaysia-yet/> accessed 1 June 2025.

framework, focusing on the **Computer Crimes Act 1997**, **Communications and Multimedia Act 1998** and **Personal Data Protection Act 2010**.

### 5.1 Computer Crimes Act 1997

The **Computer Crimes Act 1997** (hereinafter referred to as the "**CCA**") is legislation designed to address the misuse of computers in Malaysia. Its provisions criminalise conduct such as unauthorised access to computer material,[68] unauthorised access with intent to facilitate the commission of further offences,[69] and unauthorised modification of computer contents.[70]

While it was a significant milestone for Malaysia that hacking activities and the planting of malware were criminalised as early as 2000, concerns have arisen in recent years regarding the adequacy of the **CCA** in addressing modern forms of cybercrime.

**Restrictive Definition of 'Computer'**

Firstly, **Section 2** of the **CCA** defines a 'computer' in a relatively restrictive manner:

> *An electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility.*

Although the Long Title of the **CCA** states that it provides for offences relating to the misuse of computers, the definition of "computer" does not take into account the evolving nature of technologies.[71] In today's digital era, computers are no longer the only tools exploited by

[68] Computer Crimes Act 1997, s 3.
[69] *Ibid*, s 4.
[70] *Ibid*, s 5.
[71] Sovitra Sukahut Som, 'Loopholes in Malaysian Cyber Laws' (*Richard Wee Chambers*, 7 September 2022) <https://www.richardweechambers.com/loopholes-in-malaysian-cyber-laws/ > accessed 7 August 2025.

cybercriminals; offenders may utilise other technologies, devices, networks, and platforms that do not neatly fall within the statutory definition. This restrictive definition creates uncertainty as to whether newly developed devices or ICT facilities fall within the scope of the Act.

This point is well illustrated by the Singaporean case of ***PP v Muhammad Nuzaihan Bin Kamal***,[72] where the accused was convicted under the **Singaporean Computer Misuse Act 1993** for unauthorized access to computer material and unauthorised modification of computer contents. The "computers" involved were proxy servers, which fell within Singapore's broader statutory definition. By contrast, had this case occurred in Malaysia, the accused would likely have been acquitted, as proxy servers do not satisfy the conjunctive requirements imposed by the **CCA**.[73] This highlights the restrictive nature of Malaysia's statutory definition and underscores the urgent need for legislative reform to ensure that modern technologies are adequately captured under the Act.

**Outdated and Ineffective Framework**

Although the **CCA** came into force decades ago, on 1 June 2000, it has never been revised. This makes it outdated, as it cannot address modern forms of cybercrime such as DeepFake technology. The Act still reflects the computing practices of the 1990s and leaves unresolved questions concerning applications involving cloud computing, mobile devices, and Internet of Things (IoT) systems.[74] Such gaps create opportunities for cybercriminals to exploit loopholes.[75]

Besides that, the **CCA** has often faced criticism for not providing specific provisions on cybercrimes such as online fraud and phishing. Instead, it is said that the **Penal Code** governs these offences. However, this is problematic because the **Penal Code** was never designed with cybercrime in mind, and its provisions do not adequately reflect the nature of technology-based offences.

[72] [2000] 1 SLR 34.
[73] Sovitra Sukahut Som (n 70).
[74] Nur Hanan Aqilah Binti Tajul Ashikin, 'Legal Perspectives on Cybercrime in Malaysia' (*Record of Law*, 25 April 2025) <https://recordoflaw.in/legal-perspectives-on-cybercrime-in-malaysia/> accessed 18 August 2025.
[75] 'Malaysia's Cybercrime Law Reform Underway: Notes from the CYDES 2025' (*Tribute*, 5 July 2025) <https://sonnyzulhuda.com/2025/07/05/malaysias-cybercrime-law-reform-underway-notes-from-the-cydes-2025/?utm> accessed 22 August 2025.

**Disproportionate and Lenient Penalties**

It has also been criticised by N. Laidey in his article 'The Analysis of Computer Crimes Act 1997 in the Deterrence and Prevention of Computer Crimes in Malaysia' that the punishments, both fine and imprisonment term, of **CCA** are too lenient and inflexible, which ultimately undermines the law's deterrent effect. This is because, firstly, the maximum fine of RM150,000 remains capped regardless of the actual harm or loss caused by the offence. Consequently, an offender is liable only up to this ceiling, even if the financial losses or damage caused far exceed this amount. In addition, the maximum term of imprisonment under the **CCA** is 10 years, which is comparatively lower than the 20-year maximum provided under the USA's **Computer Fraud and Abuse Act 1986**.

### 5.2 Communications and Multimedia Act 1998

The **Communications and Multimedia Act 1998** (hereinafter referred to as the '**CMA**') serves as the main legislation regulating Malaysia's communications and multimedia industries. In 2025, the amended **CMA** came into force, introducing significant revisions to several provisions, including **Section 211**, which prohibits the provision of indecent content, and **Section 233**, which addresses the improper use of network facilities, or cyberbullies.[76]

**Uncertainties Arising from Incomplete Provisions**

Previously, **Section 211** made it an offence for any content applications service provider, or any other person, to provide content that was 'indecent', 'obscene', 'false', 'menacing', or 'offensive' in nature with the intent to 'annoy', 'abuse', 'threaten' or 'harass' another person, without providing any definitions for these elements. In the amended version, the provision now applies exclusively to content applications service providers, and the term 'offensive' has been replaced with 'grossly offensive'. Nevertheless, the essential elements of the

[76] Natasha L Jayasinghe, Khong Ling Qi and Maisarah Afifah Azunan, 'LEGAL REVIEW: LAW GOVERNING CYBERBULLYING AND CYBER ATTACKS IN MALAYSIA' (*Azmi & Associates*, 15 November 2024) <https://amcham.com.my/wp-content/uploads/Legal-Review-Law-Governing-Cyberbullying-Cyber-Attacks-in-Malaysia.pdf> accessed 21 August 2025.

offence remain undefined, creating continued uncertainty and potential inconsistency in the law's application.

**Restriction of Freedom of Speech**

With respect to **Section 233**, the earlier provision criminalised any person who knowingly made, created, or solicited, and initiated the transmission of any communication that was 'obscene', 'indecent', 'false', 'menacing', or 'offensive' in character, with the intent to 'annoy', 'abuse', 'threaten', or 'harass' another person. Similar to **Section 211**, the amended version substitutes the term 'offensive' with 'grossly offensive', and broadens the scope by replacing the phrase 'or harass another person' with 'harass or commit an offence involving fraud or dishonesty against, any person'. However, unlike **section 211**, the provision now provides further explanation on what constitutes 'obscene', 'indecent', 'false', 'menacing', and 'offensive' content.

Notwithstanding the amendments to the **CMA**, criticism that it restricts freedom of speech and expression continues, particularly through **Section 211** and **Section 233**, which are criticised for employing vague and overbroad terms.

Firstly, **Section 211** continues to ignore calls for giving clear definitions of the elements of the offence, leaving the provision open to arbitrary interpretation. Secondly, although **Section 233** introduces explanations clarifying the types of prohibited content, it has also sparked controversy due to the expansiveness of its wording. For example, **Explanation 1** describes 'obscene content' as material that evokes 'a feeling of disgust due to lewd portrayal'; **Explanation 2** characterises 'indecent content' as material that is 'profane in nature', **Explanation 5** defines 'menacing content' as that which causes 'evil threats' and **Explanation 6** includes 'crude references' and 'hate speech' as forms of 'grossly offensive' content. As such, the **CMA** is criticised for encroaching upon freedom of speech, as these ambiguous terms may be misapplied to suppress an individual's expression.[77] Therefore, while curbing cybercrime is crucial at this juncture, the **CMA** must be reviewed to ensure the protection of the people's constitutional right to freedom of speech.

[77] Fahmi Reza, 'Malaysia: Halt the repressive amendments to the Communications and Multimedia Act' (*Article 19*, 3 December 2024) <https://www.article19.org/resources/repressive-amendments-communications-multimedia-act/ > accessed 19 August 2025.

**Conflicting Provisions under the Act**

Besides that, recently, the Court of Appeal in ***Heidi Quah Gaik Li vs Government of Malaysia*** identified another flaw in **Section 233**.[78] The court held that criminalising offensive speech merely on the basis that it is intended to 'annoy' others effectively grants authorities the power to censor online expression, including speech that only certain groups may find objectionable due to social sensitivities. This, in turn, undermines the guarantee in **Section 3(3)** of the **CMA**, which explicitly provides that 'nothing in this Act shall be construed as permitting the censorship of the internet'.[79] In simple words, the provisions in the Act contradict one another.

### 5.3 Personal Data Protection Act 2010

The **Personal Data Protection Act 2010** (hereinafter referred to as the '**PDPA**') is the legislation that governs the protection of personal data in Malaysia. The purpose of this Act is to safeguard individual's privacy and to ensure that personal data is handled in a lawful and transparent manner.[80] Notably, however, it only regulates personal data processed in the course of commercial transactions.

**Exemption to Government**

Pursuant to **Section 3(1)** of the **PDPA**, both Federal and State Governments enjoy a 'blanket exemption' from the Act, despite being among the nation's largest consumers of personal data.[81] This highlights the inadequacy and unfairness of the Act's protection, as governments should not be privileged. Consequently, individuals are deprived of the right to take legal action when their personal data handled by government agencies are misused or mishandled.

---

[78] 'Court strikes words 'annoy'' & 'offensive'' from Communications and Multimedia Act 1998' (*The Vibes.com*, 19 August 2025) <https://www.thevibes.com/articles/news/111756/court-strikes-words-annoy-offensive-from-communications-and-multimedia-act-1998 > accessed 22 August 2025.

[79] 'Malaysia: Review the Communications and Multimedia Act now' (*Article 19,* 19 August 2025) <https://www.article19.org/resources/malaysia-review-the-communications-and-multimedia-act-now/ > accessed 23 August 2025.

[80] Jimmy Chin, 'PDPA 2010: Essential Information for Malaysian Companies' (*Cloud MSP*, 29 August 2023) <https://www.qloud.my/pdpa-2010-essential-information-for-malaysian-companies/ > accessed 20 August 2025.

[81] Sovitra Sukahut Som (n 67).

Indeed, there have been multiple significant data breaches involving government agencies.[82] For example, in 2022, the personal information of 22 million Malaysian voters was leaked from the Malaysian Election Commission website, exposing sensitive details such as full names, identification numbers, addresses, and photographs, which were subsequently sold illegally in the marketplace. In addition, a similar incident occurred when data belonging to 22.5 million Malaysians were later put on sale after being obtained from the National Registration Department's MyIdentity API.

In this context, it can be argued that the government's exemption under the **PDPA** runs contrary to the Act's objective of safeguarding individuals' personal data.

**Exclusion of Non-Commercial Activities**

Not only does the **PDPA** exempt government agencies, it also excludes all non-commercial activities from its protection. This is because it only covers commercial transactions, such as the supply or exchange of goods or services, agency, banking and finance.[83]

As such, individuals are left vulnerable when their personal data is mishandled or leaked by other platforms or organizations. In this regard, the author concurs with Murugason R. Thangaratnam, CEO of the cybersecurity company Novem CS, who stated that the **PDPA** is toothless in addressing threats in today's and the future digital world.[84] Many online websites and social media platforms, where people constantly share personal information, fall outside the purview of the Act, yet they remain susceptible to data breaches. For instance, in 2021, the personal data of 533 million Facebook users was published online for free, which included the data of 11.6 million users from Malaysia. Consequently, every Facebook user in Malaysia faced an increased risk of scams.[85] Despite the serious consequences, individuals have no legal recourse under the **PDPA**, as such incidents are considered non-commercial activities and thus not covered by the Act.

---

[82] Iman Muttaqin, 'PDPA outdated and toothless, say experts' (*The Sun*, 15 June 2022) <https://thesun.my/home-news/pdpa-outdated-and-toothless-say-experts-XE9336473 > accessed 24 August 2025.
[83] Personal Data Protection Act 2010, s 4.
[84] Iman Muttaqin (n 78).
[85] Hamzah Nazari, 'Personal Data Of 11 Million M'sians Made Public From FB But Here's How To Check' (*The Rakyat Post*, 7 April 2021) <https://www.therakyatpost.com/tech/2021/04/07/private-data-of-11-million-msians-leaked-from-fb-heres-how-to-check/ > accessed 25 August 2025.

**Lack of Civil Remedies**

Although a contravention of the **PDPA** may attract prosecution and result in criminal liability, namely fines, imprisonment, or both, aggrieved individuals are not granted any civil remedy under the Act. This means they cannot claim compensation for damages caused by a data controller's violation of statutory obligations. Instead, victims are limited to filing a civil action to recover losses suffered as a consequence of the misuse of their data.[86]

## 6.0 Conclusion

In conclusion, AI plays a dual role in the realm of cybercrime. It serves as a powerful tool for combating threats, yet provides new avenues for exploitation by criminals simultaneously. While Malaysia's three primary cyber laws offer a basic framework for regulating cybercrime, they remain riddled with loopholes that limit their effectiveness in the face of evolving AI-driven threats. It is therefore imperative that the legislature undertakes a careful and comprehensive review of these laws, introducing targeted reforms to expand their scope, strengthen penalties, and address emerging technologies. Only through such review can Malaysia's legal system remain effective in safeguarding society against the evolving risks of AI-driven cybercrime.

[86] Andrew Yoon and Joyce Ong, 'Common FAQs- Is Our Personal Data Protected?' (*Low & Partners*) <https://www.lowpartners.com/pdpa-personal-data-protected/ > accessed 24 August 2025.