ASL
Adnan Sundra & Low

LEGAL UPDATE: KEY HIGHLIGHTS OF THE CYBERCRIMES BILL 2026

MONTH :

September 2026

BY :

Sri Sarguna Raj, Steven Cheok, Nicole Chong & Syuhaini Safwan

LEGAL UPDATE: KEY HIGHLIGHTS OF THE CYBERCRIMES BILL 2026

Introduction

Malaysia's **Cybercrimes Bill 2026** ("the Bill") was passed by the Dewan Rakyat on 1 July 2026 and by the Dewan Negara on 20 July 2026, replacing the **Computer Crimes Act 1997**. The Bill will come into force on a date to be specified after it receives Royal Assent and is published in the Federal Gazette. Its key features include establishing a Committee on Combatting Cybercrimes, criminalising of specific acts involving computer systems, and strengthening investigative and enforcement powers relating to the investigation and prosecution of cybercrime offences.

Key Highlights

(1) Extra-territorial application of offences

- **Section 2** provides that offences committed outside Malaysia may be prosecuted as if committed locally if the affected computer system or data is connected to Malaysia, or if the victim is a Malaysian citizen.
- Implications: The Bill broadens the extra-territorial application of cybercrime offences, allowing offences affecting Malaysian citizens abroad to be dealt with under Malaysian law. It also removes the restriction under the repealed **Computer Crimes Act 1997** that prevented subsequent proceedings from being instituted against the same person for the same offence outside Malaysia.[1] This may give authorities more scope to address cross-border cybercrimes.

(2) Establishment and Role of the Committee on Combatting Cybercrimes

- **Section 4** stipulates the establishment of Committee on Combatting Cybercrimes ("the Committee"), a cross-agency task force involving various ministries, agencies and departments.
- Functions of the Committee, as stated under **Section 5** includes: -
  - to plan, formulate and decide on approaches and strategies in preventing and combating cybercrimes;
  - to advise and make recommendations to the Government on policies and strategic measures;
  - to coordinate initiatives among the enforcement agencies;

[1] Computer Crimes Act 1997, s 9.

- to assess and oversee the effectiveness of existing actions and mechanisms;
- to identify gaps and recommend improvements in the legal and enforcement framework; and
- to perform any other functions necessary or incidental to achieving the purposes of the Act.

- The Committee may establish any subcommittee to assist the Committee in the performance of its functions[2] and may invite any person to attend Committee meetings and advice on any matter under discussion.[3]
- Implications: Under the repealed **Computer Crimes Act 1997**, there was no central coordination committee to deal with digital threats. The Committee brings together representatives from several sectors, including –
  - National governance and security agencies (e.g. Chief Secretary to the Government, Director General of National Security);
  - Legal and enforcement agencies (e.g. Attorney General, Inspector-General of Police);
  - Digital, communications and data governance authorities (e.g. Personal Data Protection Commissioner, Chairman of the Malaysian Communications and Multimedia Commission); and
  - Financial and economic sector regulators (e.g. Governor of Bank Negara, Chairman of the Securities Commission).

The Committee is intended to improve coordination in formulating strategies, implementing preventive measures and strengthening enforcement mechanisms against cybercrimes.

[2] Cybercrimes Bill 2026, s 8.
[3] Cybercrimes Bill 2026, s 7.

(3) **Offences Relating to Confidentiality, Integrity and Availability of Computer Systems and Computer Data**

- **Sections 10** to **15** of the Bill penalises persons who: -
  - Gain unauthorised access to computer system intentionally and without authority or lawful purpose,[4] or with the intention of committing or facilitating the commission of a further offence involving fraud or dishonesty;[5]
  - Unlawfully intercept non-public computer data transmissions by technical means without lawful authority;[6]
  - Unlawfully interfere with computer data that seriously hinders or disrupts the functioning, lawful use or operation of a computer system;[7]
  - Engage in unauthorised dealing in devices, programs, passwords, access credentials, electronic signatures or similar computer data intended to facilitate the commission of offences under the Bill.[8]
- Implications: These provisions go beyond the repealed **Computer Crimes Act 1997**, which focused mainly on unauthorised access to computer material. The Bill protects the confidentiality, integrity and availability of computer systems and computer data, not just access controls.

(4) **Offences Relating to Computer-related Forgery and Computer-related Fraud**

- In relation to fraud and forgery, **Section 16** prohibits the intentional and unauthorised alteration of computer data resulting in inauthentic computer data, where such data is intended to be considered or acted upon as authentic. **Section 17** further criminalises such alteration with fraudulent or dishonest intent where it causes loss of property to another person.
- Implications: These offences align with international standards on

[4] Cybercrimes Bill 2026, s 10.
[5] Cybercrimes Bill 2026, s 11.
[6] Cybercrimes Bill 2026, s 12.
[7] Cybercrimes Bill 2026, s 14.
[8] Cybercrimes Bill 2026, s 15.

computer-related forgery and fraud, including **Articles 7 and 8 of the Convention on Cybercrime (Budapest Convention)**. They also address concerns arising from digital tampering and technology-enabled financial crimes.

(5) Offences Relating to the National Digital Identity Services

- To safeguard Malaysia's digital identity ecosystem, **Section 19** makes it an offence for a user to disclose their national digital identity password or provide access credentials, knowing or having reasonable grounds to know that doing so facilitates the commission of an offence under any written law.
- **Section 20** also penalises transmitting or making available the credentials of any user for the purpose of committing or facilitating any offence under any written law.
- Implications: **Sections 19 and 20** provide specific protection for the national digital identity service, MyDigital ID, which is the electronic identity verification and authentication service owned by the Federal Government.[9] The Bill also creates a rebuttable presumption of knowledge under **Section 19** lowering the evidential burden in offences involving the misuse of government credentials for national digital identity services. Given that MyDigital ID is integrated with various government digital services, including MySejahtera, MyJPJ, MyPTPTN and BUDI95,[10] so these provisions strengthen the legal protection of Malaysia's digital identity ecosystem.

(6) Other Cybercrime-related Offences

The repealed **Computer Crimes Act** primarily addressed unauthorised access to computer systems. The Bill covers a wide range of conduct.

- **Section 21** criminalises the unauthorised communication or disclosure of computer systems access credentials.
- **Section 22** prohibits identity theft and the unauthorised possession or use of another person's identity data to commit an offence.

[9] Cybercrimes Bill 2026, Explanatory Statement, Item 23.
[10] Izzat Hakimi, 'Senarai 36 Aplikasi & Portal Yang Kini Menyokong MyDigital ID' (MyDigital ID, 4 November 2025) <https://digital-id.my/articles/senarai_36_aplikasi_n_portal> accessed 24 July 2026.

- **Section 23** penalises the creation and distribution of any generated or manipulated media intended to deceive and facilitate the commission of an offence.
- **Section 24** outlaws the dissemination of intimate images of any person produced by any means, with heavier penalties imposed when dissemination is intended to intimidate or cause harm.
- **Section 25** extends the abovementioned protection against offences under **Part III or IV**, or **Section 21, 22 or 23 of the Bill** to National Critical Information Infrastructure Entity and National Critical Information Infrastructure.
- Implications: The Bill addresses a broader range of unauthorised conduct facilitated by technology, including manipulated digital content, identity misuse and other emerging cyber-enabled harms. The offences relating to manipulated content address the misuse of generative artificial intelligence and other forms of digital manipulation. The Bill also extends protection to National Critical Information Infrastructure ("**NCII**") and NCII Entities. Cyberattacks on essential infrastructure may affect public safety and national security as well as individual victims.

(7) Broader Enforcement Powers of Authorised Officers

- **Section 26** provides that any public officer or officer of the Commission may be authorised in writing to exercise enforcement powers under the Act.
- In addition to the general search and seizure powers, authorised officers are also empowered under **Sections 38** and **39** to require a person in possession or control of a computer system, to preserve or disclose computer data reasonably required for investigation. The recipient must comply with the written notice and maintain its confidentiality, failing which they commit an offence punishable under the Bill.
- Under **Sections 40 and 41**, service providers may be compelled to assist law enforcement in collecting real-time electronic evidence within their existing technical capabilities for cybercrime investigations. This duty extends to recording real-time

traffic data by technical means,[11] as well as intercepting, retaining, and collecting specified communications or content data.[12]

- Authorised officers are also granted broad investigative powers under **Sections 41** to **45** of the Bill, for example: -
  - To enter any premises to install, remove and retain any device necessary for communications or content data;[13]
  - To issue a written order requiring attendance of any acquainted persons;[14]
  - To examine any acquainted person orally;[15]
  - To compel the production of computer systems, computer data, storage media, documents or other relevant materials for the purposes of inspection, examination or copying;[16]
  - To require the production of identification documents;[17]
  - To make such inquiries as may be necessary for the purposes of an investigation.[18]
- **Section 48** extends the procedural powers under the Bill to investigations of offences committed by means of a computer system under any written law and to the collection of electronic evidence for the purposes of any investigation or proceedings relating to an offence under any written law.
- Implications: The Bill gives authorised officers investigative powers that reflect the electronic evidence-gathering standards in **Articles 16 to 21 of the Convention on Cybercrime (Budapest Convention)** and **Articles 25 to 30 of the United Nations Convention Against Cybercrimes**. It also includes mechanisms requiring individuals and service providers to cooperate in specified circumstances. These procedural and evidence-

[11] Cybercrimes Bill 2026, s 40.
[12] Cybercrimes Bill 2026, s 41.
[13] Cybercrimes Bill 2026, s 41(2).
[14] Cybercrimes Bill 2026, s 42(1).
[15] Cybercrimes Bill 2026, s 43.
[16] Cybercrimes Bill 2026, s 45(1)(a).
[17] Cybercrimes Bill 2026, s 45(1)(b).
[18] Cybercrimes Bill 2026, s 45(1)(c).

gathering powers apply not only to cybercrimes but also to any crime committed via a computer system.

(8) Establishment of an Integrated Information System

- Under **Section 50**, the Chief Executive of the National Cyber Security Agency (NACSA) may by written notice, request any person or Government Entity to provide any information relating to cybercrimes for the purposes of preventing and investigating cybercrimes. Such information obtained may be maintained and managed through an integrated information system, where the Chief Executive may disclose, or share any information contained therein with any Government Entity.
- Implications: The Bill expands the role of the Chief Executive of National Cyber Security Agency ("**NACSA**") beyond national security governance to include cybercrime matters. The Chief Executive of NACSA also serves as the Secretary of the Committee established under the Bill. The Chief Executive already manages the National Cyber Coordination and Command Centre System ("**NC4**") established under the **Cyber Security Act 2024**.[19] Because the Bill does not expressly cross-reference NC4, it is presently unclear whether the database contemplated under the Bill is distinct. Clarification may therefore be needed on whether the Bill establishes a separate database or is intended to utilise or expand the existing NC4 system.

(9) Expansion of Judicial Powers

- **Section 49** confers jurisdiction on the Sessions Court to try any offence committed under the Bill.
- **Section 54** empowers the Court, upon an application by the Public Prosecutor to grant various orders in relation to contraventions of the Bill. These include orders to:
  - Restrain or cease the contravention;
  - Require remedial or mitigative action including restitution against an aggrieved party;
  - Compel compliance with statutory obligations or court orders;
  - Restrict dealings with property; and

[19] Cyber Security Act 2024, s 11.

- ➢ Make any ancillary orders necessary to give effect to such orders.

- Implications: **Section 49** is consistent with the Sessions Court's existing jurisdiction under **Sections 63** and **64** of the **Subordinate Courts Act 1948**, allowing offences under the Bill to be tried and punished. **Section 54** also empowers the Court to grant preventive and remedial orders in addition to criminal penalties.

(10) Duties of Service Providers

The Bill introduces a statutory compliance framework for service providers, with preventive obligations, data retention requirements and duties to cooperate with cybercrime investigations and enforcement.

- **Section 3** adopts a broad definition of a service provider, encompassing a person, whether licensed under the **Communications and Multimedia Act 1998** or not, that offers computer communication services, processes or stores computer data, or provides information and telecommunications services.

- Under **Section 51**, service providers have a general duty to prevent their services from being used to commit cybercrimes. They may also be required to take specific preventive steps and actively assist authorities with enforcement measures.[20]

- **Section 52** empowers the Minister to publish an order, requiring service providers to retain specified categories of computer data for a designated period.

- **Section 53** provides for good faith immunity extended to service providers and their employees for any act or omission in the performance of the duty imposed under **Section 51**.

- Implications: The definition of "service provider" covers both licensed and unlicensed entities that provide digital communication or data-related services. It therefore includes entities involved in preventing, detecting and investigating cybercrimes. The immunity provision protects service providers and their employees from liability for actions performed in good faith under their

[20] Cybercrimes Bill 2026, s 51(2).

statutory obligations, which may encourage cooperation.

(11) Extension of Corporate Liability

- **Section 59** extends liability to officers of a body corporate who are responsible for the management of any of its affairs, making them liable for offences committed by the body corporate unless they establish the statutory defence provided under the Bill.
- **Section 60** further extends liability by attributing offences committed by an employee, agent, or the employee of an agent acting in the course of employment or on behalf of the principal to the person for whom they act, thereby imposing statutory vicarious liability under the Bill.
- Implications: The provisions place responsibility on both corporations and individuals to prevent and address cybercrimes through appropriate governance, compliance and oversight measures.

(12) Heftier Punishments under the Bill

- In relation to non-compliance with the Bill, relatively higher punishment standards have been introduced, for example: -
  - Lightest penalty: A fine not exceeding RM100,000 or imprisonment not exceeding 3 years, or both. Examples include offences under **Section 10** (unauthorised access to a computer system), **Section 13** (computer data interference), and **Section 19** (unauthorised disclosure of national digital identity credentials)
  - Heaviest Penalty: A fine not exceeding RM1 million or imprisonment not exceeding 10 years, or both. Examples include offences under **Section 17** (computer-related fraud), **Section 51** (failure of a service provider to comply with an authorised officer's written notice), and **Section 52** (failure of service provider to retain computer data).
- Implications: Higher statutory fines may deter non-compliance and encourage organisations to adopt appropriate technical security measures.

Conclusion

The **Cybercrimes Bill 2026** updates Malaysia's legal, regulatory, and enforcement response to digital threats. It repeals the **Computer Crimes Act 1997** and addresses statutory gaps, bringing domestic law closer to the international standards set out in the **Budapest Convention on Cybercrime** and the **UN Convention against Cybercrime**. The Bill would broaden extraterritorial jurisdiction, provide for multi-agency coordination through the Committee on Combatting Cybercrimes, impose compliance duties on service providers, permit real-time electronic evidence collection, and provide for corporate officer liability. These measures would help protect Malaysia's digital economy, critical infrastructure, and online populace.

This article was written by our Intellectual Property, Technology, Media, Sports, Gaming & Data Protection partners, Sri Sarguna Raj, Steven Cheok Hou Cher, Nicole Chong & Syuhaini Safwan, with the assistance of Soo An Qi, Emily Ong Wenyen and Adriana Lee (Managing Associate, Associates & Pupil). It contains general information only. It does not constitute legal advice or an expression of legal opinion and should not be relied upon as such.