# Malaysia: The Cybercrimes Bill 2026 is a threat to freedom of expression and the right to privacy

**ARTICLE 19, the Centre for Independent Journalism (CIJ), and Sinar Project are concerned about the threat posed by the Malaysian Cybercrimes Bill 2026 to the right to freedom of expression online, as well as to media, journalists and human rights defenders. Although Malaysia is a signatory to the United Nations Convention against Cybercrime, the current Bill does little to meet the Convention's human rights safeguards and procedural guarantees. Importantly, Article 6 of the Cybercrime Convention makes clear that States Parties to the Convention shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law. The Malaysian Cybercrimes Bill fails to provide human rights safeguards or to respect human rights and fundamental freedoms, especially freedom of expression and the right to privacy.**

On 22 June 2026, the Cybercrime Bill 2026 was tabled for first reading in Parliament by Deputy Prime Minister Datuk Seri Dr Ahmad Zahid Hamidi. The Bill covers offences including identity theft, computer-related fraud and forgery, transmission of manipulated content, and dissemination of intimate images. It will replace the Computer Crimes Act 1997.

We are very concerned about the Bill, as it could serve as a tool for government censorship of online expression. This legislation is introduced against a backdrop of existing censorship and an increasingly repressive environment for online discourse in Malaysia. This includes prosecuting dissent and targeting media, journalists, human rights defenders, and ordinary users under the Communication and Multimedia Act 1998 (CMA), the Cybersecurity Act, and the Online Safety Act (ONSA). The Bill's vague language and broad scope significantly increase the risk of misuse, thereby further restricting online freedom of expression and censoring dissent in the country. It would

give the government expansive, largely unaccountable control over computer-related activities and grant sweeping search-and-seizure powers.

**In our preliminary analysis**, we have identified several areas of serious concern from an international law perspective. Our concerns focus not only on content and computer-related offences but also on the lack of adequate human rights and procedural safeguards, such as: it lacks prior judicial authorisation for surveillance and data access, search and seizures, there are no clear limits on data retention, and it does not provide explicit protection for privileged communications, such as journalists' sources. Additionally, the investigative powers are disproportionate and excessive, the sanctions regime is inflexible, and there is no independent oversight to prevent state overreach and censorship. Collectively, these provisions risk undermining freedom of expression, privacy, due process and media freedom while exceeding what is necessary and proportionate to address legitimate cybercrime.

**In our analysis, we point out the following issues:**

1. **Significant enforcement powers without independent review or oversight**

- **Part VII of the Draft Bill sets forth numerous law enforcement powers.**
    - *Section 26* - we observe that these powers are not limited to police officers but may be conferred on any 'authorised officer', which means any police officer, public officer, or officer of the Commission (Malaysian Communication and Multimedia Commission (MCMC)) at the Minister's determination.
    - *Section 27(2)* – any person who is not a police officer may be granted 'the powers of a police officer of whatever rank as provided for under the Criminal Procedure Code' for investigating any offence under the Bill. Of particular note is that, while certain powers are granted, there is no mention of accompanying limitations or due process, qualifications, training, codes of conduct, or disciplinary procedures for these officers. It is therefore unclear whether this part effectively creates a new police designation that exercises police powers without accountability or oversight. These excessive powers are compounded by the absence of sufficiently robust procedural safeguards throughout the Bill.

We have repeatedly expressed our concerns regarding the excessive enforcement powers granted to the MCMC under various existing laws, particularly the CMA and the ONSA 2025. The further expansion of MCMC's authority through the Cybercrimes Bill

would enhance the powers of both MCMC and the communication minister, allowing them to operate without adequate oversight and effectively control and enforce censorship.

- **Section 29 – Searches and seizures do not require warrants**
    - While Section 28 sets forth criteria for a Magistrate to apply when issuing a warrant before conducting a search, Section 29 completely overrides this by offering a blanket exception to the warrant requirement. A warrant is not required if 'an authorised officer is satisfied' that 'he has reasonable cause to believe' that obtaining a search warrant under Section 28 would cause an investigation to be 'adversely affected'. All an officer must do is claim there is 'reasonable cause', and they will subsequently have all powers as if a traditional warrant had been obtained. There is no mechanism to monitor or otherwise review the self-determination of the officer. Further, the standard of 'reasonable cause' is the exact same standard that must be articulated to a judge in Section 28, meaning that an officer does not need to satisfy any heightened legal standard to skip the warrant requirement. Section 29 risks undermining the warrant requirement in Article 28 by allowing officers to bypass judicial authorisation in a wide range of cases. The Bill fails to include adequate safeguards against abuse, contravening the requirements of due process, necessity and proportionality under international law.

- **Section 36 – Officers may compel decryption**
    - Section 36 (1)&(2) allows any authorised officer conducting a search under the Bill to demand passwords, encryption or decryption codes, and software or hardware to access information. Access without thorough, independent judicial oversight violates privacy rights. We note that under international standards, encryption facilitates the exercise of free expression and privacy, and restrictions on encryption and anonymity must meet the three-part test for limitations on the right to freedom of expression under international law. Failure to comply with such a demand will be punished under Section 46 (Obstruction), which subjects the alleged offender to a fine not exceeding RM 100,000 (approximately USD 25,000), or imprisonment for not exceeding 3 years, or both. It is often the case that service providers lack the technical capacity to decrypt end-to-end communications passing through their systems; such providers should not face criminal penalties or contempt if this is the case.

Encryption facilitates the exercise of free expression and the protection of privacy. The Bill does not provide an articulated basis or standard for judicial authorisation and clear legal thresholds for issuing compelled orders, thereby empowering any officer to do so at any time. This may have grave implications for areas such as user privacy, exposure to retaliation, journalistic source protection, chilling effects on whistleblowers, the work of human rights defenders, and attorney-client confidentiality.

- **Section 38 and Section 39 – Forced preservation and disclosure of user data**
    - Sections 38 and 39 of the Bill allow officers to order the preservation and forced disclosure of user data so long as the officer is 'satisfied' that the data is 'reasonably required for the purposes of an investigation' and believes there is a risk of the data being destroyed or becoming inaccessible. These provisions do not require independent judicial notice or review, nor do they grant any right of appeal. On the contrary, Sections 38(2) and 39(2) explicitly prohibit persons issued with such a written preservation or disclosure notice from communicating the existence and content of the notice.
    - This means that those who receive such a preservation notice cannot disclose anything about it or even seek judicial oversight or remedy. It is unclear whether communicating the notice to one's legal counsel would be a violation – on its face, it would be. Thus, it may prevent or seriously impede an individual's rights to a fair trial. Failing to comply with either provision may result in a fine of 1 million ringgit (approximately USD 250,000). This sanction is disproportionately high, increases the coercive effect of the order and reinforces the chilling effect of the gag provisions.

These provisions contradict Articles 23 and 24 of the UN Cybercrime Convention, which require States to ensure that their rules and procedures protect human rights. This includes the principle of proportionality and the provision of conditions such as independent reviews, the right to an effective remedy, clear justifications for the use of these powers, and limits on their duration.

## 2. Lack of procedural safeguards

The procedural safeguards for human rights protection are markedly absent throughout the Bill. In particular, there is no reference to the obligations to uphold and protect the rights to freedom of expression and to privacy under the ICCPR. We are aware that Malaysia is not a party to the International Covenant on Civil and Political Rights

(ICCPR). Yet, in 2018 and 2021, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted that the content of Article 19 of the ICCPR is based on Article 19 of the Universal Declaration of Human Rights (UDHR) and thus should inform Malaysia's obligations under international law. We find that the absence of such provisions could threaten the Bill's overall compatibility with international human rights standards and the enforcement of human rights in this area.

- **Section 2 – Extraterritorial scope**
  - We are concerned that expanding the Bill's applicability beyond Malaysia's borders, without sufficient safeguards for a fair trial, privacy, and freedom of expression, may interfere with and violate the rights of the alleged accused and the human rights obligations of other States. This provision could also grant sweeping surveillance powers, lead to the prosecution of human rights defenders and journalists, and enable data sharing between countries with poor human rights protections and records. This could undermine legal systems and weaken trust in the justice system, threatening democratic principles. This will go against the Article 37(14) of the UN Cybercrime Convention where 'any person regarding whom proceedings are being carried out in connection with any of the offences to which this article applies shall be guaranteed fair treatment at all stages of the proceedings, including enjoyment of all the rights and guarantees provided by the domestic law of the State Party in the territory of which that person is present'.

- **Section 30 – deprives legal protections against arbitrary detention or prosecution**
  - The Bill allows that 'a search warrant issued under this Bill shall be valid and enforceable notwithstanding any defect, mistake or omission in the search warrant or in the application for such warrant' will be admissible as evidence in any proceedings under this Act. This is depriving any person of their legal protections against arbitrary detention or prosecution. Arresting or investigating anyone based on a fundamentally flawed or defective search warrant violates the right to liberty, security, and privacy and subverts the rule of law. This is against the protections guaranteed under Article 5 (fundamental liberties) and Article 8 (equality) of the Federal Constitution.

- **Insufficient protection for journalists and whistleblowers**
  - Sections 28, 29, 30, 36, 38,39 and 48 of the Bill, on access to computer systems and data, interception, interference, preservation, and disclosure of user data, when read together, allow

for the potential prosecution of journalists and whistleblowers, in violation of international standards. In many instances, anonymity is the precondition under which information is conveyed from the source to the journalist. The protection of journalists' sources is an essential element of freedom of expression. Failure to cooperate or comply with the authority's request under those provisions may lead to criminalisation and a heavy penalty.

- Section 48, which extends the powers in sections 36, 38, 39, 40 and 41 to offences under other written laws. It could be read together with the Printing Presses and Publications Act (PPPA), the Sedition Act, the CMA and ONSA, and potentially lead to overreach or mission creep.

## 3. Lack of independence or external oversight of the Committee on Combating Cybercrimes

- The Draft Bill established, in Part II, a **Committee on Combating Cybercrimes** (Committee) that raises serious concerns. Most importantly, the Committee lacks any independence at all. It is composed primarily of government agencies, with the Chief Secretary of the government serving as Chairman and the MCMC serving as Chief Executive and as the Secretariat. The addition of other members is limited to two. There are no term limits on the Committee, no external oversight or opportunity to challenge or review its composition or decisions, and no mechanisms to remove members who engage in misconduct. Any regulatory or administrative body must be independent of political interference and subject to basic procedural protections such as term limits, qualifications for admission or removal, human rights safeguards and opportunities for independent oversight.
- **Necessity and legitimacy:** At the outset, we note that a primary concern with the proposed Committee is that these approaches appear to transfer certain processes for developing internet-related standards into intergovernmental control. This shift consolidates influence over cyberspace governance and emphasises state authority over content, data flows, and surveillance, with limited meaningful participation from independent or non-state stakeholders.

- **The Chief Executive may demand production without a warrant –** This lack of independence is particularly problematic as the Chief Executive possesses significant police powers. Section 50(2) grants the power to issue written notices to 'any person' or government entity 'to provide any information relating to cybercrimes'. There is no clarity about what is meant by information here, and these notices are not subject to any external review

process and are entirely at the Chief Executive's discretion, both in substance and procedure.

## 4. Privacy under threat

### A. Sections 10, 11 and 12: Illegal access and interception

- *Section 10* criminalises the intentional and unlawful access to a computer system. The provision is overly broad and does not include a reference to the need for security measures to have been infringed or 'dishonest' intent to 'obtain computer data' to have occurred. For instance, accessing computer data without authorisation to test whether data stored in a computer system is secure could inadvertently be criminalised. The sanction would be on conviction, and the offender would be liable to a fine not exceeding RM 100,000 (approximately 25,000 USD), imprisonment for a term not exceeding three years, or both.
- *Section 11* criminalises the intentional and unlawful access to a computer system with the intention of committing fraud or dishonesty to commit a further offence. This provision is similar to Section 4(3) of the Computer Crimes Act 1997, but the penalty has been increased disproportionately from RM 150,000 (approximately 36,000 USD) to RM 500,000 (approximately 120,000 USD).
- *Section 12* criminalises the intentional and unlawful interception by technical means of non-public transmissions of computer data. Again, we note the absence of a requirement that any intent be dishonest and the failure to distinguish between lawful and unlawful interception. The sanction would be on conviction, and the offender would be liable to a fine not exceeding RM 500,000 (approximately 120,000 USD), imprisonment for a term not exceeding seven years, or both.

### B. Sections 13 to 16: Illegal data and computer system interference, misuse of device and computer-related forgery and computer-related fraud

- *Section 13* criminalises the unauthorised interference with computer data. We note with concern, however, that there is no requirement under section 13 that such modification or interference should cause serious harm or damage to a particular interest or computer data. This is not in line with Article 9(2) of the UN Cybercrime Convention. We are concerned that Section 13, in its current form, lacks a

definition of ‘computer system’ and allows them to exploit the ambiguity in their prosecution. Meaning that individuals can be prosecuted even for minor modifications that only marginally impair the operation of computer systems or other interests, in the absence of dishonest or malicious intent. It carries a fine not exceeding RM 100,000 (approximately 25,000 USD), imprisonment for a term not exceeding three years, or both.

- *Section 14* criminalises the unlawful hindrance or interference with the functioning or usage of a computer system. Section 3 defines Computer Data without properly defining Computer System, which features in this section. The provision is unduly broad because it does not require that serious harm result from the commission of an offence. The lack of a definition of ‘computer system’ allows them to exploit the ambiguity in their prosecution. It carries a fine not exceeding RM 500,000 (approximately 120,000 USD), imprisonment for a term not exceeding seven years, or both.
- *Section 15* criminalises the unlawful dealing in or possession of a device, including a computer program, password, access credentials, or electronic signature, for the purpose of committing an offence. Section 15 is overly broad and too vague in its wording. It criminalises the mere possession of a device that is capable of 'committing an offence.' This is not in line with Article 11(2) of the UN Cybercrime Convention, which stipulates that the article does not impose criminal liability for obtaining, producing, selling, distributing, or possessing the items if these actions are not meant to commit an offence or break the law. It carries a fine not exceeding RM 500,000 (approximately 120,000 USD), imprisonment for a term not exceeding seven years, or both.
- *Section 16* criminalises intentional and unlawful computer-related forgery. We welcome the inclusion of the requirement of intentionality within this Section. However, to conform with international human rights standards, the Section should include a requirement that any intention to commit forgery be dishonest before criminal liability attaches. It carries a fine not exceeding RM 500,000 (approximately 120,000 USD), imprisonment for a term not exceeding seven years, or both if it involves ‘valuable security’. In other cases, it carries a fine not exceeding RM 300,000 (approximately 72,000 USD) imprisonment for a term not exceeding five years, or both.

**5. Content-related offences**

- *Section 23* of the Bill criminalises ‘any person who transmits, distributes, publishes, sells or offers for sale or otherwise makes available, any visual or audio content generated or manipulated, whether wholly or partly, by means of a computer system’, will be liable for a fine not exceeding RM 500,000 (approximately 120,000 USD) and imprisonment for a term not exceeding 7 years, or both. While we acknowledge serious concerns about

AI-generated deepfake videos and images, such broadly framed offences relating to AI-generated content risks have negative consequences for freedom of expression, potentially criminalising creators of legitimate forms of expression, including satire, artistic works, journalism, or comments critical of the government. This concern is especially significant in Malaysia, where those who create satire and dissent continue to be targeted and legally harassed.

- *Section 24* of the Bill criminalises the dissemination of intimate images by anyone who transmits, distributes, publishes, sells, or offers for sale any intimate images, and will be liable for a fine not exceeding RM 300,000 (approximately 72,000 USD) and imprisonment for a term not exceeding 5 years, or both. The provision addresses a broad range of issues already covered by existing laws, such as the CMA. Moreover, it fails to distinguish between Child Sexual Abuse Material (CSAM) and consensual and non-consensual intimate images. It appears that it also criminalises pornography in general. The UN Cybercrime Convention addresses these in detail as separate issues under Articles 14, 15, and 16.

**6. Duty and liability of service providers**

This Bill mandates that telecommunications service providers and social media companies proactively and systematically collect, monitor and intercept substantial amounts of user data, without requiring judicial authorisation. These companies are then required to store this data for several years, under the premise that it may be needed for future criminal investigations involving specific individuals.

- *Section 40* criminalises service providers who fail to comply with the requirement to collect, record and provide real-time collection of traffic data communications that the Public Prosecutor 'considers that any traffic data associated with specified communications transmitted by means of a computer system is relevant for the purposes of any investigation' with a fine of not exceeding 1 million ringgit (approximately 240,000 USD). The designation and subsequent demands would not be subject to judicial authorisation, external review or meaningful rights of appeal. Similarly, Internet Service Providers (ISPs) and social media companies are legally bound by the CMA and are expected to comply with unreasonable demands to surveil all digital activities occurring on their systems, given the financial penalty for non-compliance. This will inadvertently provide the service providers with a strong incentive to over-censor or surveil their users to limit their

liability exposure. This is particularly true given the vague concepts and lack of safeguards and protection under the Bill.

- *Section 41(1)* criminalises service providers who fail to comply with intercepting content data, and who collect or record any specified or real-time communications that the Public Prosecutor 'considers that any communication is likely to contain content data which is relevant for the purposes of any investigation'. The designation and subsequent demands would not be subject to judicial authorisation, external review or meaningful rights of appeal.
- *Section 41(2)* allows the Public Prosecutor to authorise any officer to enter any premises to install interception devices for the interception, retention, collection, and recording of communication or content data. The designation and subsequent demands would not be subject to external review or meaningful rights of appeal. As set forth above, this would trigger numerous affirmative obligations on the part of service providers, as well as overreach into investigatory powers that would interfere with journalistic activities; for example, such interception powers may enable access to confidential communications, metadata and personally identifiable information. It appears that there is a high potential for systemic surveillance capability rather than isolated interception.

Sections 40 and 41 appear to confer power upon a service provider to remove information, terminate or suspend services and notify appropriate law enforcement agencies of any alleged illegal activity. In its current form, these provisions place the onus on the service provider to determine what constitutes illegal activity. The government should not delegate censorship measures to intermediaries. Additionally, the widespread collection and processing of data enable accurate conclusions to be drawn about individuals' daily habits, movements, regular places of residence, social connections, and other personal details. This practice is excessive and disproportionate, violating people's rights to privacy and data protection.

**Derivative, corporate, and vicarious liability**

- Section 59 of the Bill provides criminal liability for the director, compliance officer, partner, manager, secretary or 'other similar officer of the company,' where an offence under Part III of the Bill is committed by a body corporate. Section 60 provides for vicarious liability for employers for the acts of their employees or agents. We note that similar mechanisms of corporate criminal liability under Section 244(1) of the CMA have previously been used to target senior executives in media organisations. Under the provisions, employers could be held liable and

charged for the actions of their employees; thus, the editors of a news outlet would face legal exposure for their publication's reporting or its sources, thereby having a chilling effect and encouraging self-censorship. Finally, Section 59(b) provides that officers of a company or partnership are presumed to be guilty of an offence that the body corporate is convicted of unless the officer can prove the offence was committed without his knowledge or that it was committed without his consent and the officer had taken all reasonable steps to prevent the offence. Here, the corporate officer is presumed to be guilty. The usual criminal burden of proof is thus reversed, and the accused company is obliged to prove its innocence. This legal position is unacceptable in a criminal law context.

**7. Disproportionate sanctions:** In general, the Bill imposes a disproportionate and inflexible sanctions regime. The sanctions, more often than not, lack any *mens rea* requirement of dishonest intent, or any requirement that serious harm should flow from the commission of an offence before criminal liability attaches; contrary to best practices in international law. We observe that financial and custodial sanctions are imposed throughout the Bill. Moreover, a harm test or the availability of public interest defences is not provided within the Bill where appropriate.

**Recommendations**

Any legislation aimed at regulating cybercrime must prioritise the protection of the right to privacy as stipulated under Article 17 of the ICCPR. Additionally, it must adhere to the standards of freedom of expression set out in Article 19 of the ICCPR. However, this Bill raises serious concerns about its alignment with these principles and fails to meet the minimum standards set out in the UN Cybercrime Convention. It lacks adequate safeguards for the protection of human rights, including due process provisions, which creates an environment prone to overreach and misuse.

**Once more, we urge the Malaysian government to reverse the current approach and uphold freedom of expression and the right to privacy. Specifically, we call on the government to:**

1. **Halt the second reading of the Bill and send the Bill to the Parliament Special Select Committee on Human Rights, Elections, and Institutional Reform for further review and consultation to address the shortcomings identified above to ensure the compatibility of any cybercrime legislation with international standards of freedom of expression.**

2. **The Malaysian Cybercrime Bill must include clear human rights protections and safeguards that balance security and fundamental rights. The Bill must be aligned with international human rights standards, particularly freedom of expression, data protection, and the right to privacy.**
3. **Commit to transparent and inclusive policymaking by conducting thorough and meaningful public consultations with all the relevant stakeholders, especially human rights advocates and organisations, to foster trust and accountability.**
4. **Renew its commitment to human rights by signing and ratifying the International Covenant on Civil and Political Rights (ICCPR), as well as other major international human rights treaties, and by repealing or amending all laws that restrict freedom of expression in Malaysia.**

We stand ready to provide further assistance in this process.