The Legal 500 Country Comparative Guides

Malaysia: Technology

This country-specific Q&A provides an overview to technology laws and regulations that may occur in Malaysia.

For a full list of jurisdictional Q&As visit here

Contributing Firm

Shin Associates

Authors

Jessie Tan
Partner
The Legal 500
jessie@shinassociates.com.my

Joel Prashant
Senior Legal Associate
The Legal 500
joel@shinassociates.com.my

1. **What is the regulatory regime for technology?**

   There is no single authority which has an overarching purview on the regulatory regime for technology in Malaysia. The said regime is broadly governed by the following ministries and governmental agencies which have different and sometimes overlapping roles in regulating technology:

   (a) The Ministry of Energy, Science, Technology, Environment & Climate Change ("**MESTECC**") regulates exploring, developing and utilising science, technology and innovation to increase commercialization of technology, generate knowledge, create wealth, increase labour productivity, and ensure social wellbeing towards achieving a competitive, sustainable and inclusive high income economy;

   (b) The Ministry of Communications and Multimedia ("**MCM**") regulates matters relating to information technology and is tasked with determining policies and regulations in respect of the same. The Malaysia Digital Economy Corporation Sdn Bhd ("MDEC"), an agency established under the MCM, is responsible for developing, coordinating and promoting Malaysia's digital economy, information and communications technology industry as well as to promote the adoption of digital technology amongst Malaysians;

   (c) The Ministry of Finance ("**MOF**") is tasked with the responsibility for government expenditure, revenue raising, developing economic policies and preparing the Malaysian federal budget. The MOF also oversees financial legislation and regulation. Various bodies under the auspices of the MOF have significant regulatory purview over financial technology in Malaysia, such as the Securities Commission Malaysia ("SC") which regulates digital asset exchanges and initial coin offerings in Malaysia, and the Central Bank of Malaysia / *Bank Negara Malaysia* ("**BNM**") which issues currency, acts as banker and adviser to the Malaysian government and also regulates financial technology activities involving banking, investment banking, insurance or *takaful*, money changing, remittance, operating a payment system or issuing payment instrument businesses In Malaysia.

2. **Are communications networks or services regulated?**

   Communications networks and services in Malaysia are regulated under the Communications and Multimedia Act 1998 ("**CMA**") and its subsidiary legislation.

3. **If so, what activities are covered and what licences or authorisations are required?**

   Persons who own or provide network facilities ("**Network Facilities Providers**"), persons who provide network services ("**Network Service Providers**"), persons who provide applications services ("**Applications Service Providers**") and persons who provide applications services which provide content ("**Content Application Service Providers**") require licences under the CMA, which are separated into licences for individuals and by classes.

4. **Is there any specific regulator for the provisions of communications-related services?**

   The Malaysian Communications and Multimedia Commission ("**MCMC**"), established by the Malaysian Communications and Multimedia Commission Act 1998 ("**MCMCA**"), specifically regulates the provision of communications-related services in Malaysia and is empowered to supervise, regulate and enforce legislation relating to communications and multimedia-related activities and is entrusted with:

   (a) Advising the Malaysian government on all matters concerning national policy objectives for communications and multimedia activities;

   (b) Making recommendations to the Malaysian government on various matters, including the grant of individual licences, cancellation of a person's registration under a class licence, and variations of licence conditions;

   (c) Implementing and enforcing the CMA;

   (d) Issuing directions in writing to any person regarding compliance with licence conditions, including the remedy of a breach of a licence condition, the CMA or its subsidiary legislation;

   (e) Holding public inquiries in relation to proposed changes to regulation; and

   (f) Issuing determinations on mandatory standards for matters subject to a voluntary industry code.

5. **Are they independent of the government control?**

   The MCMC is not independent of government control as the Minister of Communications and Multimedia ("**Minister**") is empowered to regulate the MCMC under the CMA and the MCMCA.

6. **Are platform providers (social media, content sharing, information search engines) regulated?**

   In general, platform providers are not regulated in Malaysia. Only telecoms operators which carry out the functions of Network Facilities Providers, Network Services Providers, Applications Service Providers and Content Applications Service Providers are regulated as provided in the CMA.

7. **If so, does the reach of the regulator extend outside your jurisdiction?**

Notwithstanding that the MCMC does not have jurisdiction outside of Malaysia, Section 269 of the CMA provides that the Minister may direct the MCMC regarding the interworking arrangements between the MCMC and any other authority in Malaysia or in a foreign jurisdiction, or any international organization.

8. **Does a telecoms operator need to be domiciled in the country?**

Telecoms operators carrying out the functions of Network Facilities Providers, Network Services Providers, Applications Service Providers and Content Applications Service Providers will need to apply for an individual licence or a class licence under the CMA. In order to be eligible for such licences, in terms of domicile and foreign ownership, the applicant must be a Malaysian-incorporated company and the shareholding of the licensee company must comply with Malaysian foreign investment restrictions. With respect to market access, commercial presence in Malaysia is established through the incorporation of local joint venture companies with Malaysian individuals or Malaysian-controlled companies or through the acquisition of shares of existing licensed operators. Foreign companies are generally ineligible for licenses under the CMA.

9. **Are there any restrictions on foreign ownership of telecoms operators?**

The shareholding of a licensee must comply with relevant Malaysian foreign investment restrictions. Foreign equity restrictions are commonly imposed as licence conditions in practice and such restrictions apply to all licences issued under the CMA, except for Applications Service Provider licences, which can be 100% foreign-owned.

10. **Are there any regulations covering interconnection between operators?**

The CMA is the principal legislation for interconnection and access to facilities and services between operators. The establishment of an access regime under the CMA enables providers to obtain access to necessary facilities and services on reasonable terms and conditions.

Section 228 of the CMA provides that a Network Facilities Provider must provide non-discriminatory access to any post, pole, tower, or other above-ground facilities for carrying, suspending or supporting any network facilities (“Post”), network facilities or right-of-way. However, access may be denied in certain situations, such as where there is insufficient capacity, or for reasons of safety, security, reliability, or difficulty of a technical or engineering nature, as long the reason for the denial of access is not due to discrimination.

Network Facilities Providers and Network Service Providers are required to provide access to their network facilities or services listed in the access list under the CMA to any other Network Facilities Providers, Network Services Providers, Applications Service Providers and Content Applications Service Providers. Network Facilities Providers and Network Service Providers have to prepare a Reference Access Offer Agreement for each facility listed in the access list. The Access Provider has disclosure, negotiation, content and service obligations

under the MCMC's Determination on the Mandatory Standard on Access or under any determinations of MCMC.

Any written agreement between providers for access to listed facilities and services must be registered with the MCMC in order to be enforceable.

11. **If so are these different for operators with market power?**

The MCMC is empowered to direct a licensee in a "dominant position" in a communications market to cease conduct in that communications market which has, or may have, the effect of substantially lessening competition in any communications market, and to implement appropriate remedies.

The MCMC-issued Guideline on Dominant Position, read together with the Competition Act 2010 ("**Competition Act**") provides that in analysing whether a licensee is in a dominant position in a relevant communications market, the MCMC will consider the structure of the market and nature of competition in that market, including market shares; barriers to entry and expansion; countervailing power of buyers; and nature and effectiveness of economic regulation (if any). It should be noted that although the Competition Act does not govern the exercise by the MCMC of its powers under the CMA, the MCMC considers that the definition of a market under the Competition Act provides guidance in defining communications markets for the purposes of the CMA.

The effect of access regulation under the access list will be considered by the MCMC in order to determine whether a licensee is being sufficiently constrained in a communications market. The existence of access regulation will not prevent a licensee from being in a dominant position if it does not provide an effective constraint on the ability of a licensee to act independently in a market. Access regulation may only constrain the activities of licensees in relation to particular products supplied in a market rather than more generally in the market.

If the MCMC considers that a provider is in a dominant position, it may direct the provider to cease conduct that substantially lessens competition in the communications market.

12. **What are the principal consumer protection regulations that apply specifically to telecoms services?**

Under Section 188 of the CMA, all Network Facilities Providers, Network Services Providers, Applications Service Providers and Content Applications Service Providers (save for those who are not required to have individual or class licenses or are exempted from licence requirements) are required to deal reasonably with consumers and adequately address consumer complaints, on pain of a fine not exceeding RM20,000 or to imprisonment for a term not exceeding 6 months or to both upon conviction.

The MCMC-issued General Consumer Code of Practice for the Communications and Multimedia Industry in Malaysia ("**Code**") forms the principal consumer protection regulation for telecommunication services in Malaysia and binds all service providers licensed under the CMA insofar as their licensed activities are concerned as well as members of the consumer forum established under the CMA.

The Code aims to provide model procedures on reasonably meeting consumer requirements, the handling of customer complaints and disputes, the use of alternative dispute resolution, procedures for the compensation of customers in the event the Code is breached, and the protection of consumer information, amongst others. The Code also seeks to achieve the relevant national policy objectives of the CMA, provide benchmarks for the communications and multimedia service providers for the benefit of consumers, promote a high level of consumer confidence in the delivery of services from the industry, and provide guidelines for self-regulation among industry players.

Consumers of telecommunications services would also enjoy protection vide the Consumer Protection Act 1999 ("**CPA**") and the Consumer Protection (Electronic Trade Transactions) Regulations 2012 which impose disclosure requirements pertaining to the goods and services offered by a business and the identification details of that business, and prohibiting misleading practices and representations by businesses to consumers.

13. **What legal protections are offered in relation to the creators of computer software?**

Computer software enjoy copyright protection under the definition of "literary works" pursuant to the Copyright Act 1987 ("**CA**").

Pursuant to Section 36A of the CA, creators of computer software may protect their copyright in their work via the application of technological protection measures to a copy or copies of their work. Except for very limited circumstances, the CA prohibits any person from circumventing, causing, or authorising any other person to circumvent such technological protection measures:-

(a) which are used by the creators in connection with the exercise of their rights under the CA; and

(b) which restrict acts in respect of his/her works which are not authorized by the owner concerned or permitted by law.

The High Court in **Creative Purpose Sdn Bhd & Anor v Integrated Trans Corp Sdn Bhd & Ors [1997] 2 MLJ 429** decided that the modification of computer software programmes to circumvent the security features of the software amounted to copyright infringement even if it was done without direct copying of the original programme.

If a software invention involves hardware and/or a technical effect or solves a technical problem in a novel and non-obvious manner, it may also be protected by patent rights, although the patentability of software in Malaysia remains unclear. To date, the Intellectual Property Corporation of Malaysia ("**MYIPO**") has not prescribed any guidelines for the examination of software-based inventions.

14. **Do you recognise specific intellectual property rights in respect of data/databases?**

There are no definitions as to what a "database" or "database right" constitutes, or any specific case laws addressing the extent of protection afforded to databases. Compilation of data in a database will either be recognized and enjoy copyright protection as a literary work under the head of "tables and compilations" under Section 3 of the CA, which includes in particular "*tables or compilations, whether or not expressed in words, figures or symbols and whether or not in a visible form*", or as a derivative work under Section 8 of the CA by virtue of being a collection of works protected by copyright or data which constitute intellectual creation due to the selection and arrangement of their contents.

15. **What key protections exist for personal data?**

The Personal Data Protection Act 2010 ("**PDPA**") and its subsidiary legislation regulates the processing of personal data in commercial transactions and applies to anyone who processes and has control over or authorises the processing of any personal data in respect of commercial transactions.

The PDPA establishes 7 key principles which must be complied with by data users when processing personal data: (i) consent; (ii) notice and choice; (iii) disclosure; (iv) security; (v) retention (vi) data integrity; and (vii) access. The PDPA also requires data users to have adequate security and indemnity measures to inhibit the theft, misuse, unauthorized access, accidental disclosure, alteration or destruction of personal data under their care.

Codes of practice may be implemented by various data user forums or the Personal Data Protection Commission for various classes of users in differing sectors. These codes of practice would have a binding effect on the various classes of users registered with the Personal Data Protection Commission.

Following the implementation of the European Union's General Data Protection Regulation ("**GDPR**"), the Malaysian government is reviewing the PDPA to comply with international requirements on personal data protection, including the GDPR. However, there is no definite timeframe for the implementation of updates to the PDPA.

16. **Are there restrictions on the transfer of personal data overseas?**

A data user shall not transfer any personal data of a data subject to a place outside Malaysia

unless specified by the Minister, upon the recommendation of MCMC or, by notification published in the Gazette.

Notwithstanding the above, a data user may transfer personal data out of Malaysia in the following circumstances:

(a) “the data subject has given his consent to the transfer;

(b) the transfer is necessary for the performance of a contract between the data subject and the data user;

(c) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which:-

(i) is entered into at the request of the data subject; or

(ii) is in the interests of the data subject;

(d) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;

(e) the data user has reasonable grounds for believing that in all circumstances of the case—

(i) the transfer is for the avoidance or mitigation of adverse action against the data subject;

(ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and

(iii) if it was practicable to obtain such consent, the data subject would have given his consent;

(f) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of this Act;

(g) the transfer is necessary in order to protect the vital interests of the data subject; or

(h) the transfer is necessary as being in the public interest in circumstances as determined by the Minister.”

17. **What is the maximum fine that can be applied for breach of data protection laws?**

Non-compliance with the PDPA may result in the organisation, upon conviction, being liable to a fine ranging from RM100,000 to a maximum of RM500,000 and/or to imprisonment ranging from 1 to 3 years.

18. **What additional protections have been implemented, over and above the GDPR requirements?**

The PDPA has yet to be amended to address the GDPR requirements its implementation. No additional protections have been implemented in Malaysia since the coming into force of the GDPR and the GDPR presently imposes stricter requirements in comparison. For example:

(a) Consent

PDPA: Does not define what 'consent' entails save that consent collected has to be in a form that can be maintained by the data user and any consent obtained should be presented distinguishable from consent given for other matters. The collection of consent by way of an "opt-out" method is permitted under certain circumstances.

GDPR: "consent" has to be freely given, specific, informed and unambiguous indication of the data subject's wishes by a statement or a clear affirmative action. The "opt-out" method of obtaining consent may not apply to the GDPR.

(b) Data Protection Officer

PDPA: Requires data users to identify a contact person in a data protection notice, for data subjects to direct any queries they may have regarding the use of their personal data. There is no requirement to specifically appoint a data protection officer under the PDPA.

GDPR: Certain organisations are required to specifically appoint a data protection officer to, inter alia, act as a liaison to data subjects in respect of issues relating to the processing of personal data.

(c) Data Breach & Reporting

PDPA: Does not impose any obligation on data users to report data breaches to the Commissioner.

GDPR: Data controllers are obliged to report data breaches to the appropriate supervising authority within 72 hours, and to the relevant data subjects if the breach is likely to result in a high risk to the rights of the data subject.

(d) Right to be Forgotten / Right to Erasure

PDPA: Does not grant data subjects a right to be forgotten or right to erasure, although they may withdraw their consent for the processing of their personal data. While the effect of such withdrawal is unclear, the exercise of such right may require the data user to delete the personal data of the data subject.

GDPR: If a data controller is requested by a data subject to erase the data subject's personal data, the data controller must comply with the request without delay unless the situation falls within an exemption.

(e) Data Portability

PDPA: Provides that data subjects may request for their information from a data user, however, it is unclear on the manner/method/medium in which such information is to be given. It does not provide data subjects with a right to request for their personal data to be transferred to different data users.

GDPR: Data subjects have a right to request for their information held by a data controller to be provided to them in a machine-readable form. Data subjects may also request for their personal data to be transferred from one data controller to another in certain circumstances.

However, where the personal data of children is to be processed, the PDPA imposes stricter requirements, in that the personal data of children under the age of 18 may only be processed after consent is given by the child's parent/guardian, as opposed to children under the age of 16 as required by the GDPR.

19. **Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?**

There is currently no legislation specific to cloud-based services in Malaysia, and such services may be subject to other legislation depending on the services provided, in particular:

(a) cloud-based service providers which provide or intend to provide cloud-based services would need to determine whether the cloud-based services would fall under any of the licensing requirements of the CMA. The different types of licences prescribed under the CMA are addressed in Question 1.2 and licensing requirements would vary from different cloud-based service providers. The MCMC in October 2018 registered a technical code on Information and Network Security – Cloud Service Provider Selection ("**CSPS Code**") which seeks to set out the requirement for network interoperability and the promotion of safety of network facilities by specifying the requirements for selecting cloud service providers for organisations in ensuring all security requirements are taken into account based on the

assessment of the current environment and objectives. While compliance with the CSPS Code is not in itself mandatory, the MCMC is empowered to direct a person or a class of persons to comply with the CSPS Code. Failure to comply with such directions by the MCMC may result in a fine of up to RM200,000 being imposed;

(b) financial institutions which intend to use data services or cloud services providers outside of Malaysia to deliver cloud services are required to seek approval from BNM in accordance with BNM's Policy Document on Outsourcing (which came into force on 1 January 2019) and BNM's Guidelines on Data Management and Management Information System Framework for Development Financial Institutions; and

(c) cloud-based service providers would fall under the purview of the PDPA as "data users – a person who either alone or jointly or in common with other persons processes any personal data, or has control over or authorises the processing of any personal data" as the act of "processing" has been defined in the PDPA to include "storing of personal data". Cloud-based service providers storing personal data using cloud-based services would have to ensure that they comply with the provisions of the PDPA.

20. **Are there specific requirements for the validity of an electronic signature?**

Save for transactions involving powers of attorney, wills, and codicils, trusts and other negotiable instruments, the Electronic Commerce Act 2006 ("**ECA**") applies to commercial transactions conducted through electronic means.

Section 9(1) of the ECA provides that "Where any law requires a signature of a person on a document, the requirement of the law is fulfilled, if the document is in the form of an electronic message, by an electronic signature which—

(a) is attached to or is logically associated with the electronic message;

(b) adequately identifies the person and adequately indicates the person's approval of the information to which the signature relates; and

(c) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required."

Section 9(2) of the ECA further states that "For the purposes of paragraph (1)(c), an electronic signature is as reliable as is appropriate if—

(a) the means of creating the electronic signature is linked to and under the control of that person only;

(b) any alteration made to the electronic signature after the time of signing is detectable; and

(c) any alteration made to that document after the time of signing is detectable."

The ECA further provides that the Digital Signature Act 1997 ("**DSA**") continues to apply to any digital signature used as an electronic signature in any commercial transaction. A digital signature is defined under the DSA as "a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine (a) whether the transformation was created using the private key that corresponds to the signer's public key and (b) whether the message had been altered since the transformation was made."

Section 62(1) of the DSA specifically prescribes that:

"Where a rule of law requires a signature or provides for certain consequences in the absence of a signature, that rule shall be satisfied by a digital signature where—

(a) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;

(b) that digital signature was affixed by the signer with the intention of signing the message; and

(c) the recipient has no knowledge or notice that the signer—

(i) has breached a duty as a subscriber; or

(ii) does not rightfully hold the private key used to affix the digital signature."

Section 66 of the DSA also provides that a certificate issued by a licensed certification authority shall be an acknowledgment of a digital signature verified by reference to the public key listed in the certificate if that digital signature is (a) verifiable by that certificate; and (b) affixed when that certification was valid.

21. **In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?**

The Guidelines on Information Security in ICT Outsourcing published by CyberSecurity Malaysia (an agency under the MCM) ("**Outsourcing Guidelines**") states: "*Before outsourcing, an organisation is responsible for the actions of all their staff and liable for their actions. When these same people are transferred to an outsourcer they may not change desk*

but their legal status has changed. They no longer are directly employed or responsible to the organisation. This causes legal, security and compliance issues that need to be addressed through the contract between the client and suppliers. This is one of the most complex areas of outsourcing and requires a specialist third party adviser."

The Outsourcing Guidelines advise that the organization ought to ensure that security requirements and processes to protect organizational assets ought to be incorporated into the formal agreement entered into with the outsourcing supplier and upon complete performance of the outsourcing agreement, the outsourcing supplier is responsible for returning all borrowed assets and the organization should ensure that "*all assets borrowed and used by the outsourcing provider during the outsourcing project are returned promptly*".

Notwithstanding the advisory nature of the Outsourcing Guidelines, the treatment and status of employees, assets and/or third-party contracts would typically also be addressed in the outsourcing agreement and may not be automatically transferred.

22. **If a software program which purports to be a form of A.I. malfunctions, who is liable?**

There is no specific legislation regulating artificial intelligence ("**AI**") in Malaysia. Software programmes with a form of AI would be treated similarly to other consumer products. In the event of a malfunction, liability would be addressed by the Sale of Goods Act 1957 ("SOGA"), CPA and the law of torts, which collectively serve as a platform for product safety and consumer protection.

The Contracts Act 1950 ("**Contracts Act**"), which serves to address the rights and liabilities of parties pursuant to a contract, would be relevant in determining liability for AI malfunctions. In a contract relating to the use of an AI, provisions may be included to determine which of the parties will sustain liability arising out of AI malfunctions.

Section 68(1) of the CPA states that "where any damage is caused wholly or partly by a defect in a product, the following persons shall be liable for the damage:

(a) the producer of the product;

(b) the person who, by putting his name on the product or using a trade mark or other distinguishing mark in relation to the product, had held himself out of the producer of the product; and

(c) the person who has, in the course of his business, imported the product into Malaysia in order to supply it to another person."

The SOGA and the CPA impose several implied terms which cannot be excluded by contract when dealing with consumers. These include implied guarantees and conditions regarding title and lack of encumbrances, correspondence with description, satisfactory or acceptable quality, fitness for purpose, price, and repairs and spare parts. The AI software manufacturer or supplier will be liable for any malfunction that results in a breach of these mandatory implied terms, depending on the extent of non-compliance with the representations and guarantees made by the manufacturer to the supplier and the supplier to the consumer respectively regarding the AI software programme.

Manufacturers may rely on the "development of risk" defence to exonerate liability by demonstrating that apart from observing the industrial standard, the scientific and technical knowledge at the relevant time disabled any attempts of discovering the defect. However, the strict liability rule introduced in the CPA will have a significant bearing in negating the defence. Manufacturers and/or suppliers may also be found liable for AI software malfunctions under the tort of negligence.

If an AI is tasked with creating content and malfunctions by incorporating third-party works protected by copyright in such content without authorisation, the liability for such infringement pursuant to the SOGA, CPA, Contracts Act, and law of torts would accrue to the creator of the AI, subject to any contractual provisions addressing liability between the creator and the user of the AI for such infringement occasioned by the AI.

However, with rapidly growing development of AI such as the introduction of Google Duplex, AI may no longer be a mere product, but one capable of human mimicry and potentially gaining legal personality, consciousness, personhood, authorship and autonomy. In such event, the legal position on AI would drastically change.

23. **What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?**

A) obligations as to the maintenance of cybersecurity?

There is currently no single legislation governing cybersecurity. In April 2019, the Malaysian government indicated that it is studying the possibility of introducing an Act on cybersecurity, however no definite timeframe has been set for its development. The current legislation applicable to cybersecurity are:

(a) Computer Crimes Act 1997 ("**CCA**"): The CCA provides for offences relating to the misuse of computers and applies if the computer, programme or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time. The act(s) of gaining unauthorized access into computers or networks, committing or facilitating the commission of further offences, unauthorized modification of the contents of any computer and/or wrongful communication are all offences under the CCA and depending

on the offence, upon conviction, applicable fines range from RM25,000 to RM150,000 and/or imprisonment of 3 to 10 years.

(b) CMA: The CMA was enacted to provide for and to regulate the converging communications and multimedia industries and regulates network facilities, network services, applications services, content applications services and includes the prescription of the licensing framework relating to such services and the activities undertaken by licensees thereunder. Section 263(1) of the CMA prescribes that "A licensee shall use his best endeavour to prevent the network facilities that he owns or provides or the network service, applications service or content applications service that he provides from being used in, or in relation to, the commission of any offence under any law of Malaysia." The CMA prohibits inter alia the fraudulent or improper use of network facilities or network services; the use and possession of counterfeit access devices; the use of equipment or devices to obtain unauthorized access to any network services; and interception of any communications except with lawful authority.

(c) CA: It is an offence under Section 36A of the CA to circumvent (or the cause or authorization thereof) of any technological protection measure that is applied to a copy of copyright work. Technological protection measure is defined as "any technology, device or component that, in the normal course of its operation, effectively prevents or limits the doing of any act that results in an infringement of the copyright in a work". The CA also expressly prohibits anyone from (a) designing, producing, adapting or performing for the purpose of enabling or facilitating the circumvention of technological protection measure; and (b) to manufacture, import or sell any technology or device for the purpose of circumventing any technological protection measure.

(d) Penal Code ("**PC**"): Where specific cybersecurity-related offences are not captured under the CCA, CMA or CA, the PC which codifies most criminal offences and procedures in Malaysia, may be relied on to prosecute such offences.

(e) PDPA: The PDPA applies to any person who processes and has control over or authorises the processing of any "personal data" in respect of commercial transactions. There are 7 data protection principles that form the basis of protection under the PDPA, one of which is the Security Principle. Pursuant to Section 9(1) of the PDPA, a data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access of disclosure, alteration or destruction. In addition to the provisions of the PDPA, the Regulations also require data users to develop a security policy to ensure that personal data is protected from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. The Department of Personal Data Protection published the Personal Data Protection Standard which enumerates the minimum security standards for personal data processed electronically and non-electronically. The SC on 31 October 2016 also published Guidelines on Management of Cyber Risk making it mandatory for entities to have clear and comprehensive cyber policies and procedures which are commensurate with their risk profiles.

(f) Strategic Trade Act 2010 ("**STA**"): As part of Malaysia's international obligations on national security, the STA controls the export, transhipment, transit and brokering of strategic items and technology, including arms and related materials, as well as activities that will or may facilitate the design, development, production and delivery of weapons of mass destruction. Section 7 of the STA provides that the Minister of International Trade and Industry may, by order published in the Gazette, prescribe any items as strategic items for the purposes of the STA.

(g) Other Applicable Guidelines or Regulations: The National Cyber Security Policy ("**NCSP**") was implemented by the Malaysian government with the aim to develop and establish a comprehensive programme and a series of frameworks to ensure the effectiveness of cybersecurity controls over vital assets and various sectors comprising the Critical National Information Infrastructure ("**CNII**"). While there are generally no minimum protective measures required, the Malaysian government has stipulated ISO/IEC 27001 Information Security Management Systems as the basis for information security standards and has proposed for all CNII sectors to be appropriately certified. There are also sector-specific guidelines that deal with cybersecurity in Malaysia. These include the Data Management and Management Information System Framework and Guidelines on Internet Insurance issued by the Central Bank of Malaysia.

B) What key laws exist in terms of the criminality of hacking/DDOS attacks?

A. Hacking

Hacking, being the unauthorised intrusion into or control over computer network security systems for some illicit purpose, is encapsulated in Section 3(1) of the CCA which provides that

"*A person shall be guilty of an offence if—*

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that is the case."

Section 4 of the CCA further provides that:

"(1) *A person shall be guilty of an offence under this section if he commits an offence referred*

to in section 3 with intent—

(a) to commit an offence involving fraud or dishonesty or which causes injury as defined in the Penal Code [Act 574]; or

(b) to facilitate the commission of such an offence whether by himself or by any other person.

(2) For the purposes of this section, it is immaterial whether the offence to which this section applies is to be committed at the same time when the unauthorized access is secured or on any future occasion."

A person found guilty of an offence under Section 3 of the CCA is liable to a fine not exceeding RM50,000 and/or imprisonment not exceeding 5 years while a person found guilty of an offence under Section 4 of the CCA is liable to a fine not exceeding RM150,000 and/or to imprisonment for a term not exceeding 10 years.

Hacking is also a criminal offence under the CA in respect of the circumvention (or the cause or authorisation thereof) of any technological protection measure that is applied to a copy of a copyrighted work. Section 41(1)(h) of the CA provides that "*any person who during the subsistence of copyright in a work or performers' right circumvents or authorizes the circumvention of any effective technological measures referred to in subsection 36A(1) shall, unless he is able to prove that he had acted in good faith and had no reasonable grounds for supposing that copyright or performers' right would or might thereby be infringed, be guilty of an offence and shall on conviction be liable…a fine of not less than RM4,000 and not more than RM40,000 for each contrivance in respect of which the offence was committed and/or to imprisonment for a term not exceeding 10 years and for any subsequent offence to a fine of not less than RM8,000 and not more than RM80,000 for each contrivance in respect of which the offence was committed and/or to imprisonment for a term not exceeding 20 years*".

Persons who commit hacking offences may also be penalised under the PC and other applicable legislation for other ancillary offences, which include Section 378 of the PC for taking dishonestly without consent any movable property, or dishonest misappropriation of property under Section 403 of the PC, or identity theft under Section 416 of the PC.

B. Distributed Denial of Service ("DDOS") Attack

While there is no specific legislation for DDOS attacks, Section 233(1)(b) of the CMA provides that a person who initiates a communication using any application service, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address, commits an offence.

A person found guilty of an offence under Section 233(1)(b) of the CMA is liable to a fine not exceeding RM50,000 and/or to imprisonment for a term not exceeding 1 year and shall also be liable to a further fine of RM1,000 for every day during which the offence is continued after conviction.

Additionally, Section 431A of the PC provides that a person who commits mischief by cutting or injuring any electric telegraph cable, wire, line, post, instrument or apparatus for signalling, shall be punished with imprisonment for a term which may extend to 2 years and with a fine.

24. **What technology development will create the most legal change in your jurisdiction?**

The increased global adoption of blockchain technology and AI appear to be the principal technological harbingers of legal change in Malaysia. There is no regulatory framework in place to govern the use of such technology in Malaysia but services which rely on blockchain technology to operate, such as digital asset/cryptocurrency exchanges ("**DAX**"), have seen increasing regulatory intervention from the authorities in Malaysia.

The SC has issued the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 and revised its Guidelines on Recognized Markets to introduce new requirements for DAX operators to register with the SC and obtain the SC's approval for establishing and operating such exchanges. Operating a DAX without such registration and approvals is an offence under securities laws and a person in breach may be liable to a fine or imprisonment term or both.

DAX operators are also required to register with BNM as reporting institutions under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ("**AMLATFA**"), pursuant to the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Digital Currencies (Sector 6) policy document issued by BNM. Failure to comply with BNM's requirements is an offence under the AMLATFA.

MESTECC has established a special taskforce to study the implementation of blockchain in the country as well as the Shariah compliance component thereof as it has identified that blockchain has immense potential applications across various industries, especially the Islamic finance sector. While the taskforce is presently at a nascent stage, MESTECC is determined to engage in discussions with various stakeholders on the development of blockchain and to develop a Shariah-compliant guideline for blockchain technology.

The UN Centre for Trade Facilitation and Electronic Business ("**UN/CeFact**")'s whitepaper titled, 'White Paper on the technical applications of blockchain to UN/CeFact deliverables', was brought to the attention of the Malaysian National Standards Committee on Blockchain and Distributed Ledger Technologies ("**Committee**") and the Committee has been tasked

with the development of standards and guidelines on blockchain and distributed ledger technologies in Malaysia.

Purveyors will soon be subject to greater regulation and scrutiny in the near future, and the widespread implementation of blockchain technology and AI will have a domino effect on the Malaysian legal framework. New legislation will need to be introduced and implemented, and existing legislation and regulations will need to be amended to account for the impact blockchain and AI technology have on the various industries in Malaysia.

25. **Which current legal provision/regime creates the greatest impediment to economic development/ commerce?**

Various regulatory requirements to conduct business in Malaysia often deter foreign investment into Malaysia which in return reduces economic development. Such requirements typically include corporate presence in Malaysia, and the imposition of various equity and shareholding requirements amongst others. Control over meeting these requirements is exercised twofold, in that:

(a) committees under various governmental ministries are given the task of procuring guidelines to advise on these requirements; and

(b) equity ownership is controlled through the issuance of licences, permits and employment passes or in the purchase of/acquisitions of interest in real property is enforced via administrative discretion exercised under legislative authority.

While the government has liberalised major sectors of the economy, strategic sectors of national interest will continue to be safeguarded through sector regulators.

The stringent licensing regime in Malaysia would also have a hand in restricting economic development and commerce in Malaysia. Entities engaging in commerce would need to apply for various licenses and registrations with various authorities in order to conduct business and equity conditions or restrictions may be imposed vide the issuance of such licences by the relevant authorities. Such licenses and registrations are often interconnected with time-consuming application processes and the requirement for stringent compliance with directorship and equity stipulations by the relevant authorities would need to be simplified to facilitate economic development and commerce in Malaysia.

26. **Do you believe your legal system specifically encourages or hinders digital services?**

The development and utilisation of digital services in Malaysia has been strongly advocated by the government. Specific agencies and incentives have been instituted to facilitate the development of the digital economy, such as MDEC. MDEC has set up a Digital Hub to attract technology investments, support local technology innovations and create a sustainable digital

ecosystem in Malaysia.

The government revealed various initiatives to accelerate the adoption of digital technology in Malaysia and to boost the digital economy at the 29th Multimedia Super Corridor ("**MSC**") Malaysia Implementation Council Meeting in October 2017. One initiative was the "Cloud-First" strategy, where it would introduce a method of faster delivery of information technology services such as data sharing and online transactions in which resources are retrieved from the Internet through web-based tools and applications, as opposed to direct connections to servers. Led by MDEC, the government is also developing a National AI Framework, an expansion of the National Big Data Analytics Framework.

Regulatory and governmental initiatives have been implemented and/or proposed over the past years to facilitate the development of digital services, particularly in the financial technology sector.

In 2018, the MOF launched the National Regulatory Sandbox Initiative to create a brainstorming group consisting of regulators and selected industry players to enable innovators to experiment and test their technological solutions/products which either require regulatory framework or which may potentially impact a regulatory environment in a conducive space.

The issuance of the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 by the SC and its revision of its Guidelines on Recognized Markets has smoothened the introduction of DAX operators into Malaysia and clearly sets out requirements for entities intending to operate DAX systems in Malaysia, which in turn facilitates the regulated implementation of DAX services in the country. On 4 June 2019, 3 DAX operators were approved and registered by the SC.

The implementation of the Interoperable Credit Transfer Framework by BNM has resulted in a boom of 'e-money' and 'e-wallet' systems in Malaysia, which paved the way for the expansion of cashless transactions in the Malaysian economy and interconnectivity of such systems with other digital services in Malaysia. However, venturing into the 'e-money' and 'e-wallet' business will necessitate going through significant regulatory red tape as multiple approvals and/or licenses from various bodies may be required for the same.

The Malaysian government intends to impose a service tax on digital services ("**Digital Services Tax**") which are imported by consumers in Malaysia under a business-to-customer regime with effect from 1 January 2020, to level the playing field between local and foreign digital service suppliers, and to provide an avenue for taxation of the digital economy. The Service Tax (Amendment) Bill 2019 relating to the Digital Services Tax was passed in parliament on 8 April 2019.

To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?

AI and the use of AI are not regulated in Malaysia. The development of AI has been so rapid that the law has failed to keep pace, not just in Malaysia but globally. While no laws and/or updates to existing legislation have been prepared to specifically address the myriad of legal issues associated with AI, it cannot be said that the Malaysian legal system is wholly unprepared to deal with such issues, as Malaysian product safety and consumer protection laws (which have been discussed in detail in Question 16 above) would apply to the current legal status of AI in Malaysia.

However, the Malaysian legal system is continuously evolving in terms of AI adoption and will need to improve in terms of its readiness to adopt and/or implement AI systems, and focus on all areas, particularly investment in AI adoption to accelerate its AI journey. The Malaysian government is taking steps to drive the country's AI ecosystem by pursuing the development of the National AI Framework through MDEC which would lend guidance on how AI and the legal issues associated therewith may be addressed in Malaysia.