The Legal 500 & The In-House Lawyer
Comparative Legal Guide
Malaysia: Technology

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

It will cover communications networks and their operators, databases and software, data protection, AI, cybersecurity as well as the author's view on planned future reforms of the technology market.

This Q&A is part of the global guide to Technology. For a full list of jurisdictional Q&As visit http://www.inhouselawyer.co.uk/index.php/practice-areas/technology

Country Author: Seow & Associates

The Legal 500

Jessie Tan, Partner

jessietan@seowassociates.com

The Legal 500

Cheong Shih Wen, Partner

shihwen@seowassociates.com

The Legal 500

Joel Prashant, Associate

joelprashant@seowassociates.com

The Legal 500

1. **Are communications networks or services regulated? If so what activities are covered and what licences or authorisations are required?**

   Communications networks and services in Malaysia are regulated under the

Communications and Multimedia Act 1998 (“CMA”). Persons who own or provide network facilities (“Network Facilities Providers”), persons who own or provide network services (“Network Service Providers”), persons who provide applications services (“Applications Service Providers”) and persons who own or provide applications services which provide content (“Content Application Service Providers”) require a licence under the CMA. The licences are further separated into licences for individuals and by classes.

2. Is there any specific regulator for the provisions of communications-related services? Are they independent of the government control?

The Malaysian Communications and Multimedia Commission (“MCMC”) 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. 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 Malaysian Communications and Multimedia Commission Act 1998. The MCMC is tasked with advising the Minister on all matters concerning the national policy objectives for communications and multimedia-related activities.

3. Does an operator need to be domiciled in the country? Are there any restrictions on foreign ownership of telecoms operators?

Telecoms operators which carry 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 license or a class licence under the CMA. In order to be eligible for such licenses, in terms of domicile and foreign ownership, the licensee must be a company incorporated in Malaysia and the shareholding of the licensee company must comply with Malaysian foreign investment restrictions. With respect to market access, commercial presence in Malaysia is only

established through the incorporation of local joint venture companies with Malaysian individuals or Malaysiancontrolled companies or through the acquisition of shares of existing licensed operators. Foreign companies (as defined under the Companies Act 2016) are generally ineligible for licenses under the CMA.

The Malaysian government had in 2011, announced the autonomous liberalisation of telecommunications services by allowing 100% foreign equity participation for Application Service Providers; and 70% foreign equity participation for Network Facilities Providers and Network Services Providers.

4. **Are there any regulations covering interconnection between operators? If so are these different for operators with market power?**

The CMA is the principal legislation in respect of 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.

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.

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

In respect of treatment of operators of differing market powers, under the CMA, 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 its Guideline on Dominant Position on 24 September 2014.

The Guideline on Dominant Position 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). The MCMC may derive the existence of a dominant position from either a single factor or from multiple factors, depending on the facts of the case. Where other factors that are relevant to the assessment of dominance exist in a particular market, the MCMC will also take these into account.

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.

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

Under 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.

In 2003, the MCMC issued the General Consumer Code of Practice for the Communications and Multimedia Industry in Malaysia (“Code”) which forms the principal consumer protection regulation for telecommunication services in Malaysia.

The Code 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 for reasonably meeting consumer requirements, the handling of customer complaints and disputes, the creation of alternative dispute resolution and procedures for compensation for 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 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.

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

Computer software or computer programmes enjoy copyright protection under the definition of “literary works” pursuant to the Copyright Act 1987 (“CA”). The computer programme must meet certain requirements for copyright to subsist in the programme, i.e. that sufficient effort has been expended to make the programme original in character and that the programme has been reduced to material form, amongst other requirements.

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

(b) that 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** also 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.

Provided that a software invention involves hardware and/or a technical effect or solves a technical problem in a novel and non-obvious manner, a software 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 softwarebased inventions.

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

While there is neither a definition as to what a "database" or "database right" constitutes, nor has there been specific case law addressing the extent of protection afforded to databases, the 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 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.

8. What key protections exist for personal data?

The Personal Data Protection Act 2010 ("PDPA") 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 Personal Data Protection Commissioner ("Commissioner") has also issued subsidiary legislation pursuant to the PDPA, particularly Personal Data Protection Regulations 2013 ("Regulations") and Personal Data Protection Standard 2015 ("Personal Data Protection Standard").

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

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 binding effect on the various classes of users registered with the Personal Data Protection Commission. The Association of Banks in Malaysia has issued a code of practice targeted at all banks and financial institutions licensed under the Financial Services Act 2013, the Islamic Financial Services Act 2013 and the Development Financial Institution Act 2002. The code of practice provides for inter alia (1) measures to be deployed by banks and financial institutions to ensure the non-infringement of the data subjects' rights when processing personal data; and (2) matters for the consideration of banks and financial institutions to ensure that risks to the personal data of data subjects are minimised. The Personal Data Protection Code of Practice for the Utilities Sector (Electricity), and the Personal Data Protection Code of Practice for the Insurance/Takaful Industry are also other codes of practice that have

been approved and registered by the Commissioner.

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

A data user may transfer personal data out of Malaysia only in the following circumstances provided under Section 129(3) of the PDPA:

(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."

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

The maximum fine that may be imposed under the PDPA is RM500,000.

11. Are there any 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 and licensing requirements would vary from different cloud-based service providers; and

(b) 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.

12. 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. 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 acknowledgement 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.

13. 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 Ministry of Science, Technology and Innovation) ("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.

14. If a software program which purports to be an early form of A.I. malfunctions, who is liable?

There is no specific legislation regulating artificial intelligence ("AI") in Malaysia. Software programmes with an early form of AI would be treated similarly with other consumer products. In the event of malfunction, liability would be addressed by the Sale of Goods Act 1957 ("SOGA"), Consumer Protection Act 1999 ("CPA") and law of torts, which collectively serve as a platform for product safety and consumer protection.

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.

However, with the 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. In such event, the legal position on AI would drastically change.

15. What key laws exist in terms of obligations as to the maintenance of cyber security?

While it was previously announced in June 2017 that the Malaysian Government would introduce a new law aimed at protecting Malaysians from cybersecurity threats, there

is currently no single legislation in respect of cybersecurity. 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 specifically 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 also 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 nonelectronically. The Securities Commission Malaysia 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: There are also sector-specific guidelines that deal with cybersecurity in Malaysia. These include the Data Management and Management Information System (MIS) Framework and Guidelines on Internet Insurance issued by the Central Bank of Malaysia.

16. **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 offences ancillary thereto, these 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. Denial of Service Attack

While there is no specific legislation for denial of service 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.

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.

17. 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. Currently, there is no regulatory framework in place to govern the use of such technology and related services in Malaysia.

The Malaysian Ministry of Science, Technology and Innovation ("MOSTI") has established a special taskforce to study the implementation of blockchain in the country as well as the Shariah compliance component of the technology as it has identified that blockchain has immense potential applications across various industries, especially the Islamic finance sector, and acknowledges that the technology could provide efficiencies. While the taskforce is presently at a nascent stage, MOSTI 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 Centre for Trade Facilitation and Electronic Business (UN/CeFact) deliverables' ("Whitepaper"), 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.

With the rapid implementation of blockchain technology and AI, 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.

18. 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. The requirements for certain licences would typically include the incorporation of a company in Malaysia, the imposition of various equity and shareholding requirements, minimum Bumiputera (a term which includes Malaysians with cultural affinities indigenous to the region, mainly the Malays in West Malaysia and various other indigenous natives of Sabah and Sarawak) participation in companies and/or local directorship and local workforce requirements, amongst others. Control over meeting these requirements is exercised twofold, in that (i) committees are set up under various governmental ministries and are given the task of procuring guidelines to advise on these requirements; and (ii) equity ownership is controlled through the issuance of licences, permits and employment passes or in the purchase of real property and acquisitions of any interest in real property, and Bumiputera participation is enforced via administrative discretion exercised under legislative authority.

While the government has largely liberalised major sectors of the economy, strategic sectors of national interest will continue to be safeguarded through sector regulators. Furthermore, 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. If the operations of a company or business in Malaysia require such licences and registrations, equity conditions or restrictions may be imposed vide the issuance of such licences by the relevant authorities. More often than not, these licenses and registrations are interconnected, for example, participants in the distributive trade sector require a Wholesale Retail Trade licence and ancillary business licences in order to operate, and such licenses are required before distributive trade companies can apply for work permits for foreign employees. The application processes for such licenses are time-consuming and the requirement for stringent compliance with directorship and equity stipulations by the relevant authorities would need to be streamlined and simplified to facilitate economic development and commerce in Malaysia.

19. 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. The Malaysian Economic Development Corporation ("MDEC"), an agency established under the Ministry of Finance ("MOF"), has been entrusted to develop, coordinate and promote Malaysia's digital economy, information and communications technology industry as well as to promote the adoption of digital technology amongst Malaysians. Its Digital Hub has been set up to attract technology investments, support local technology innovations and create a sustainable digital ecosystem in Malaysia.

The previous government had 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. The then government also planned to develop a National Artificial Intelligence (AI) Framework, an expansion of the National Big Data Analytics (BDA) Framework, to be led by MDEC.

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. On 18 October 2016, the Central Bank of Malaysia implemented a regulatory sandbox which aims to enable the experimentation of financial technology solutions in a live environment, subject to appropriate safeguards and regulatory requirements, to encourage and enable experimentation of solutions that utilise technology innovatively to deliver financial products or services.

On 14 February 2018, the MOF launched the National Regulatory Sandbox Initiative to create a brainstorming group consisting of regulators and selected industry players in

the agriculture, biotechnology, building, education, energy, finance, food, green technology, healthcare, hospitality, smart city, sports, telecommunications, transportation, tourism, water management and waste management sectors, 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.

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

AI and the use of AI is currently not regulated in Malaysia, by legislation or otherwise. The development of AI has been so rapid that the law has failed to keep pace, not just in Malaysia but across the globe. Currently, only product safety and consumer protection laws (which have been discussed in detailed in Question 13 above) would apply to AI.

Despite the possible introduction of the National Artificial Intelligence (AI) Framework and other similar initiatives introduced to accelerate the adoption of digital technology in Malaysia, the present laws in Malaysia are insufficient to deal with complex ethical and liability issues relating to AI such as personhood, agency, negligence, and autonomy, amongst others.