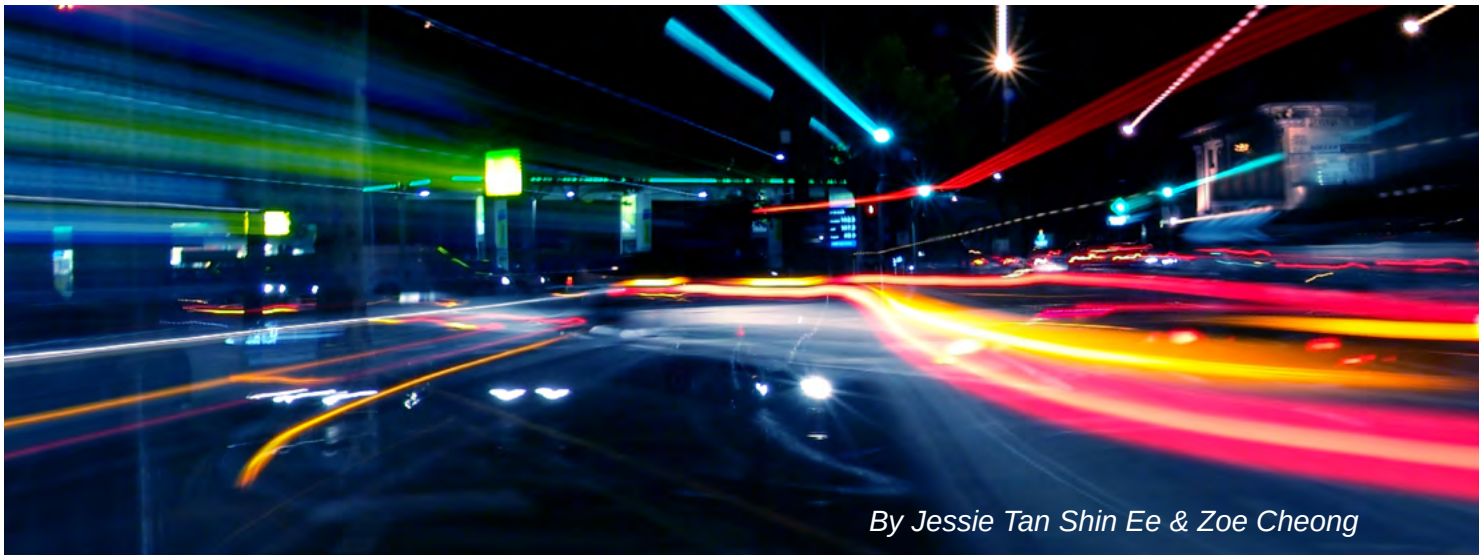
Laws and Regulations Governing Technology in Malaysia



By Jessie Tan Shin Ee & Zoe Cheong

Malaysia's technology sector is rapidly growing. Businesses today are investing in technology to gain competitive advantage over other businesses, both locally and worldwide. The Malaysian Government has been advocating the development of the technology sector and has set in place various laws and regulations to govern and grow the technology sector in Malaysia.

This article addresses the laws and regulations that Malaysia currently has in place to govern the technology sector in Malaysia, including areas such as communication networks and their operators, databases and software, data protection, artificial intelligence and cybersecurity

Communication Networks and Services in Malaysia

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 Services 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.

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 also tasked with advising the Minister of Communications and Multimedia on all matters concerning the national policy objectives for communications and multimedia-related activities.

Telecoms operators that 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 licence or a class licence under the CMA. In order to be eligible for such licences, 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 Malaysian-controlled companies, or through the acquisition of shares of existing licensed operators. Foreign companies (as defined under the Companies Act 2016) are generally ineligible for licences under the CMA.

In 2011, the Malaysian Government 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.

Databases and 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, ie 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 for 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 the technological protection measures that:

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

(b) restrict acts in respect of his/her works which are not authorised 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.

Software may also be protected by patent rights, provided that the software invention involves hardware and/or a technical effect or solves a technical problem in a novel and non-obvious manner, 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.

While there is neither a definition as to what a "database" or "database right" constitutes, nor has there been any specific case law addressing the extent of protection afforded to databases, the compilation of data in a database will either be recognised and enjoy copyright protection as a "literary work" 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: (i) works protected by copyright; or (ii) data, which constitutes intellectual creation due to the selection and arrangement of their contents.

Data Protection in Malaysia

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 seven key principles that 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, unauthorised 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 imprisonment ranging from one to three 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 a 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 *interalia:*

(a) measures to be deployed by banks and financial institutions to ensure the non-infringement of the data subjects' rights when processing personal data; and

(b) 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.

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."

It should be noted that in March 2019, the Malaysian Government announced that it is reviewing the PDPA to ensure that it is in line with new developments in the field of data protection, particularly, the EU's General Data Protection Regulations. The proposed amendments to the PDPA ("Proposed Amendments") are expected to be presented in Parliament towards the end of 2019. However, please note that the Proposed Amendments have neither been incorporated in the form of a Bill nor passed as an Act of Parliament, and thus have yet to be granted the force of law. The timeframe for passing a Bill and the coming into force of an Act of Parliament may take in excess of a year, and it is possible that the Proposed Amendments may not be implemented in 2019, if at all.

Artificial Intelligence in Malaysia

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, has held himself out to be 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 that 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.

Cybersecurity in Malaysia

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 as follows:

(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 unauthorised access into computers or networks, committing or facilitating the commission of further offences, unauthorised 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 three 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 unauthorised 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 authorisation thereof) 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: (i) designing, producing, adapting or performing for the purpose of enabling or facilitating the circumvention of technological protection measure; and (ii) 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 seven 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, unauthorised 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.

(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 Bank Negara Malaysia or the Central Bank of Malaysia. The Securities Commission has also published the "Cyber Risk Guidelines on Management of Cyber Risk", making it mandatory for entities to have clear and comprehensive cyber policies and procedures that are commensurate with their risk profiles.

Conclusion

The Malaysian Government has launched several frameworks and initiatives to accelerate the adoption of digital technology in Malaysia, such as Digital Hub launched by the Malaysian Digital Economy Corporation Sdn Bhd, National Big Data Analytics Framework, National Artificial Intelligence Framework and National Regulatory Sandbox Initiative, and will continue to do so to regulate and expand the technology sector in Malaysia.

Notwithstanding that the Government has set in place certain laws and regulations to govern the technology sector in Malaysia, the rapid development of the technology sector has far outpaced legislative efforts and this is particularly evident in the field of AI, which is currently unregulated in Malaysia, despite global developments on AI.

About the Authors

Jessie's expertise lies in the field of commercial and corporate law, employment and intellectual property laws. She has advised clients from various industries, particularly the technology, media and telecommunications ("TMT") sector. Known for her industry knowledge, Jessie has advised domestic and international film production companies making their films in Malaysia and some of the well-known productions that she has advised and worked on include "Crazy Rich Asians", "Strike Back" and "Skyfire". She also has experience in film regulatory and investment matters. In addition to handling trade mark and copyright registration matters Jessie has also advised clients on their intellectual property rights and arrangements and strategies for licensing, branding and global protection. Jessie may be contacted at jessietan@seowassociates.com.

Zoe has a vast experience in corporate, commercial, banking and finance, technology, conveyancing law and among others. Throughout her practice, she has been involved in various due diligence exercises for both foreign and local companies and advised and drafted contracts for clients from various industries. She has also been involved in the preparation of various legal documentation for various companies including start-ups, which are mostly technology companies. Zoe may be contacted at zoe@shinassociates.com.my.