LRC issues report on Cyber-Dependent Crimes and Jurisdictional Issues

The Law Reform Commission of Hong Kong (LRC) today (January 9) published a report on Cyber-Dependent Crimes and Jurisdictional Issues, recommending the introduction of a new piece of bespoke legislation on cybercrime to cover five types of cyber-dependent crimes, i.e. crimes that can be committed only through the use of information and communications technology devices, where such devices are both the tool for committing the crimes and the target of the crimes. The report represents the first part of the LRC's study on cybercrime on which the LRC's Cybercrime Sub-committee issued a consultation paper in July 2022.

The five cyber-dependent crimes are illegal access to program or data, illegal interception of computer data, illegal interference with computer data, illegal interference with computer system, and making available a device, program or data for committing a cyber-related crime (or possessing such device, program or data for the purpose of making it available). The Sub-committee, chaired by Mr Derek Chan, SC, has studied the current laws in Hong Kong and the corresponding legislation in a number of other jurisdictions, namely Australia, Canada, England and Wales, Chinese Mainland, New Zealand, Singapore and the United States of America.

At present, different computer-related offences are covered in the Crimes Ordinance (Cap 200) (CO) and the Telecommunications Ordinance (Cap 106) (TO), and some are outdated. This is unlike other jurisdictions mentioned above, which have all provided for the five cyber-dependent crimes and their related jurisdictional issues either by enacting bespoke cybercrime legislation, or dedicating a part of their codified law to cybercrime.

The responses to the consultation paper have been taken into account by the LRC in formulating the final recommendations in the report. The LRC has further observed the guiding principles of balancing the rights of netizens and the interests of persons in the information technology industry against the need to protect the public's interest and right not to be disturbed or attacked when using or operating their computer system.

Some of the main final recommendations in the report are:

(i) Unauthorised access to program or data without lawful authority should be a summary offence (Access Offence). The defendant's knowledge that the access is unauthorised is one of the key mental elements of this offence. An aggravated form of offence arises if the unauthorised access is accompanied by an intent to carry out further criminal activity. Apart from a general defence of reasonable excuse, specific defences are recommended to permit unauthorised access made for a range of specific purposes, including cybersecurity purposes, the protection of the interests of vulnerable persons (i.e. children under 16 and mentally incapacitated persons), as well as genuine educational, scientific and research purposes.

(ii) Unauthorised interception of computer data carried out for a dishonest or criminal purpose should be an offence. This offence would protect both private and non-private communications, and would apply to data generally, including metadata (i.e. information about a communication), data in transit and data momentarily at rest during transmission, and would therefore offer better protection to communications by members of the public than the existing section 27(b) of the TO, which is predicated on a telecommunications context. As "for a dishonest or criminal purpose" represents a high evidential threshold, it would not be necessary to provide any specific defence or exemption for professions or genuine businesses that intercept or use computer data in the ordinary course of their operation.

(iii) By transposing the existing provisions regarding "misuse of a computer" in sections 59(1A), 60 and 64(2) of the CO into the new cybercrime legislation, illegal interference with computer data and computer system should be offences (Interference Offences), subject to a general defence of reasonable excuse. Since access to program or data normally precedes interference with computer data or computer system, interference with computer data or computer system for cybersecurity purposes should be a specific defence in addition to the two lawful excuses specified in the existing section 64(2) of the CO (which also apply to the Access Offence).

(iv) Knowingly making available a device, program or data (or a part thereof) for committing a cyber-related crime (or knowingly possessing

such a device, program or data for the purpose of making it available) should be an offence. This offence would apply so long as the primary use of the device, program or data, determined objectively, is to commit a cyber-related offence, regardless of whether or not it can be used for any legitimate purposes. The aggravated form of the offence would occur if the perpetrator intends that the device, program or data be used (whether by himself or another person) to commit a cyber-related offence. To avoid over-criminalisation, a general defence of reasonable excuse and specific defences for cybersecurity, educational, scientific and research purposes are recommended. Further specific defences that cater to the operation of internet service providers, hosting service providers and automated technology are also available.

(v) In line with the international norm, Hong Kong law should provide for the extra-territorial application of the five proposed cyber-dependent offences. Hong Kong courts should have jurisdiction in a case where connections with Hong Kong exist. This includes cases where the perpetrator's act has caused or may cause serious damage to Hong Kong, or where the victim was physically present in Hong Kong at the time when the offence was committed.

(vi) As the severity of the harm caused by cybercrime has a wide range, each of the five proposed cyber-dependent offences has two maximum sentences in general, one applicable to summary convictions (two years' imprisonment) and the other to convictions on indictment (14 years' imprisonment). An exception is the aggravated form of the Interference Offences involving a danger to life (e.g. interference with a railway signal system). The proposed maximum penalty for it is life imprisonment which is consistent with that of the aggravated offence of criminal damage already prescribed under the current CO.

The report and its executive summary can be accessed on the website of the LRC at www.hkreform.gov.hk. Hard copies are also available on request from the Secretariat of the LRC at 9/F, Champion Tower, 3 Garden Road, Central, Hong Kong.