THAILAND – COUNTRY REPORT

Background

This report outlines the main laws which provide law enforcement and intelligence agencies with legal powers in relation to lawful interception assistance, the disclosure of communications data, certain activities undertaken for reasons of national security or in times of emergency, and censorship of communications under the laws of the Kingdom of Thailand.

Following a coup d'état on 22 May 2014, Thailand is currently governed by the interim government under the de facto control of the National Council for Peace and Order (a military junta). A state of martial law which had been imposed since the beginning of the coup was lifted on 1 April 2015 and immediately replaced by NCPO Order No. 3/2558 (3/2015) re: Maintaining Public Order and National Security issued under Section 44 of the Interim Constitution for an indefinite period of time.

Section 1 to 3 of this report summarises the laws which apply to surveillance and censorship powers in ordinary times. Section 4 explains how military rule affects the implementation of these laws on a legislative basis.

1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

1.1 Constitution of the Kingdom of Thailand (Interim) B.E. 2557 (2014) (the "Interim Constitution")

Following the coup d'état, the National Council for Peace and Order issued the Interim Constitution and repealed the Constitution of the Kingdom of Thailand 2007 (the "2007 Constitution"). The 2007 Constitution protected communications from access, interception and disclosure, but provided certain exceptions for government authorities, for example, in relation to national security or public order. As the 2007 Constitution has now been repealed, these protections are no longer guaranteed.

Section 4 of the Interim Constitution recognises that any human rights and freedoms customarily recognised in Thailand and any rights recognised under international obligations are protected under the Interim Constitution. The Interim Constitution does not explain what those rights "customarily recognised in Thailand" include.

On 7 August 2016, the referendum of the new constitution was held and the result was in support of the draft constitution. The new constitution is tentatively expected to come into effect within 2017. The new draft constitution (Section 36) still protects communications from access, interception and disclosure except in accordance with a court order or writ, or where the government has legal grounds provided by law.

1.2 Computer Crimes Act B.E. 2550 (2007) (the "CCA")

The scope of the CCA deals with offences committed against computer systems or computer data, and content offences which include the pure computer crimes and some crimes specified under the Thailand Penal Code (the "Penal Code") and committed via a computer. The CCA applies to service providers and is overseen by the Ministry of Digital Economy and Society and Computer Data Screening Committee ("MDE").

The scope of the CCA extends to those committing an offence under the CCA outside of Thailand, including both Thai and foreign citizens (Section 17 CCA). Such offenders may be penalised within Thailand.

Under section 18(4)-(8) CCA, a competent official upon obtaining the court order (one appointed by the MDE), is empowered to:

- copy computer data or traffic data from a computer system which is reasonably suspected of being used for an offence;
- inspect or access a computer system, computer data, computer traffic data or computer data storage equipment;
- order the person in possession or control of such data equipment to deliver it to him; and
- seize or attach any computer system for the purposes of gathering evidence in an investigation.

Section 18(7) CCA also authorises competent officers, upon obtaining a court order, to decrypt encrypted computer data, order concerned persons to decrypt encrypted computer data and/or to order concerned persons to cooperate with competent officers in decrypting computer data.

"Computer data" means data, statements, or sets of instructions contained in a computer system, the output of which may be processed by a computer system, including electronic data.

"Computer traffic data" means data related to computer system-based communications showing sources of origin, starting points, destinations, routes, time, dates, volumes, time periods, types of services or other information related to that computer system's communications.

Although section 18 CCA does not refer expressly to "interception", there is no judicial or statutory guidance on the MDE's powers under this section. It may be interpreted widely to include, for example, the ability to conduct direct interception, to require interception assistance or to gain direct access to a network operator or service provider's system.

Under section 19 CCA, the powers under section 18(4)-(8) may only be applied if the competent official first makes an application to the competent court.

The application must identify the grounds on which it is believed that an offender is committing or is going to commit an offence under the CCA, the reason for requesting the authority, the characteristics of the alleged offence, a description of the equipment used to commit the alleged offence and details of the offender, to the extent that this is possible.

If the court approves the application, and before taking any further action, the official must send a memorandum explaining the grounds on which the application has been granted to the owner or person in possession of the computer system. Within 48 hours of starting the operation in question, the official must also submit a copy of the memorandum and an explanation of the rationale of the operation to a court with jurisdiction.

The use of section 18(4) (copying of computer data) must not excessively interfere with or obstruct the business operation of the owner or person in possession of the computer data.

Furthermore, in relation to seizure or attachment under section 18(8), the official must issue a letter of seizure or attachment to the person who owns or possesses that computer system as evidence. The seizure or attachment must not last longer than thirty days. If a longer time period is required, a petition must be filed at a court with jurisdiction for permission to extend the time period. The court may allow several extensions, but together they must not exceed sixty days.

When that seizure or attachment is no longer necessary, or upon its expiry date, the competent official must immediately return the computer system that was seized or withdraw the attachment.

Although intercept powers may be inferred from other pieces of legislation (outlined below), the relatively simple process provided for under the CCA means that it is likely to be the legislation under which an interception is most often conducted.

1.3 Organisation to Assign Radio Frequency and to Regulate the Broadcasting and Telecommunication Services Act, B.E. 2543 (2000) (the "NBTCA")

Under the NBTCA, on the grounds of public order or public security, the National Broadcasting and Telecommunications Commission is empowered to issue a provisional order to the competent authority to seize, put to use, prohibit the use of, or prohibit the removal of, radio communication equipment, or part thereof, within the period and under the conditions specified in the order.

1.4 Special Case Investigation Act B.E. 2547 (2004) (the "SCIA")

Under section 21, powers under the SCIA may be invoked in relation to criminal cases which involve the violation of specified laws and which have particular characteristics, including those which are particularly complex, those with relevance to national interests, those involving influential people, or cases otherwise selected by the Special Case Board (the "SCB"). Such cases are referred to as Special Case Offences. The relevant laws set out in the Annex to the SCIA include violation of the Law on Loans Amounting to Public Cheating and Fraud, the Competition Act, the Public Company Act, and the Copyright Act.

The SCB is constituted under section 5 SCIA and consists of a number of government ministers and Cabinet-appointed experts chaired by the Prime Minister. Its duties are found under section 10 SCIA and include: the duty to advise the Cabinet regarding the determination of special cases, determining the details of a special offence, and the monitoring and assessment of results of compliance with the SCIA.

Under section 25 SCIA, Special Case Inquiry Officials ("SCIO") (officials working directly for the Department of Special Investigation under the Ministry of Justice) may access and acquire any documents or information sent by a means of communication or any IT media which has been or may be used to commit a Special Case Offence.

The SCIA may therefore apply to network operators and service providers if there is cause to believe that an individual being investigated for a crime under the SCIA has used their services to commit a Special Case Offence.

The SCIO must obtain a court order from the Chief Justice of the Criminal Court (the "Chief Justice") prior to the use of the powers under SCIA.

When granting a court order, the Chief Justice will consider the effect on the rights of the different parties involved and the application overall in light of the following conditions:

(a) there are reasonable grounds to believe that a Special Case Offence is or will be committed;

(b) there are reasonable grounds to believe that access to the information will result in gathering relevant information in relation to a Special Case Offence; and

(c) there are no more appropriate or efficient methods.

(d) The Chief Justice may grant permission for use of the powers for a period of up to 90 days. The network operator or service provider can be required to assist with any decryption of acquired encrypted data under the terms of the court order.

1.5 National Cybersecurity Bill (the "Bill")

The Bill is currently pending the review by the Office of the Council of State. It proposes to establish a National Cybersecurity

Committee charged with detecting and countering online threats to national security, stability, the military and economy.

Under section 35 of the Bill, the Committee would be authorised to access information on personal and other electronic devices, for the purpose of fulfilling its cybersecurity duties, in accordance with the rules and conditions specified by the cabinet. This means the access of information under section 35 does not require a court order, unless the rules and conditions specified by the cabinet provide otherwise. Please note that the details of the rules and conditions specified by the cabinet as mentioned in section 35 are not publicly known.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Computer Crimes Act B.E. 2550 (2007) (the "CCA")

Under section 18(1)-(3), for the purpose of an investigation and the gathering of evidence in relation to an offence under the CCA, a competent official (one appointed by the Minister of Digital Economy and Society) is given a range of powers including the powers to summon any person related to the offence to give a statement, to procure computer traffic data relating to the relevant communications from a service provider or from other relevant persons, and to request documents and other evidence from the person(s) concerned.

There is no requirement for a court order for use of these powers.

Under section 26 CCA, a service provider must store computer traffic data (described in section 1 above) for at least 90 days from the date on which the data is input into a computer system. However, if necessary, a relevant competent official may, on a case by case basis, instruct a service provider to store data for a period longer than 90 days but not exceeding two years.

Section 17 CCA makes it clear that the provisions of the CCA apply to offences committed outside Thailand.

Under section 22 of CCA, disclosure of personal data without prior consent from the person to which the personal data relates can be made if the disclosure is made for the purpose of prosecuting a person committing an offence under CCA or other laws (which use computer data as part of or relating to committing of criminal offences), for the benefit of prosecuting a public official on the ground of abuse of power or in relation to the unlawful exercise of their power under section 18 paragraph 2 of CCA, or disclosure under the court's order or permission.

2.2 Telecommunications Business Act B.E. 2544 (2001) (the "TBA")

The TBA is applicable to telecommunications operators. Under section 50 TBA, telecommunications licensees must keep the personal data of their service users for three months and, in the event that the service is terminated, to retain this data for three months following the date of termination of the service.

2.3 Special Case Investigation Act B.E. 2547 (2004) (the "SCIA")

Disclosure of data, including disclosure of metadata relating to customer communications, may be provided in accordance with section 25 SCIA (as described in section 1.5 above), provided that a court order is obtained first.

3. CENSORSHIP

3.1 The Cyber-Inspector Group (the "CIG")

The Ministry of Digital Economy and Society (formerly the Ministry of Information and Communication Technology) (the "MDE") was created in Thailand in 2002. One of the MDE's main priorities has been internet regulation, implemented through an MDE unit originally known as CIG. This unit monitors websites for harmful content, facilitates the enactment of legislation governing electronic transactions and conducts training for personnel to combat cyberterrorism.

3.2 Computer Crimes Act B.E. 2550 (2007) (the "CCA")

Under section 20, where information is deemed to negatively affect national security (including lèse majesté, explained below) or may violate public order or good morals (such as pornography), the authorised officials may, with the approval of the Minister of the MDE, petition the relevant court with jurisdiction to halt the dissemination of information directly or to order a service provider to do so.

Lèse majesté is an offence against the dignity of the reigning sovereign of Thailand, as well as the regent, and the crown prince/princess. Lèse majesté provisions under Thai law are included in section 2 of the Interim Constitution which stipulates that "the King shall be enthroned in a position of revered worship and shall not be violated. No person shall expose the King to any sort of accusation or action".

Lèse majesté is also classified under section 112 of the Penal Code, (Offences Relating to the Security of the Kingdom).

Section 14 CCA, also provides for a variety of offences which may be relevant to censorship, including:

(i) inputting into a computer system, with fraudulent intent, forged or false data in a manner likely to cause injury to the public which does not include the defamation;

(ii) inputting false data into a computer system in a manner likely to damage maintenance of national security, public security, national economic security or public infrastructure serving public interest in order to cause public panic;

(iii) inputting data into a computer system constituting an offence against national security under the Penal Code;

(iv) inputting any data of pornographic or obscene nature into a computer system which is publicly accessible; or

(v) disseminating or forwarding any of the above types of data in the knowledge that the inputting of such data constitutes an offence.

If the offence under paragraph one (1) has not been committed against the public, but against an individual, the person who committed such offence, the distributor or the sender of such computer data shall be subject to imprisonment not exceeding three years and a fine not exceeding sixty thousand baht, or both, and it is a compoundable offence.

Under section 15 CCA, any service provider which intentionally supports or consents to the commission of an offence under section 14 shall be sentenced to a jail term not exceeding five years and/or a fine not exceeding 100,000 Thai baht, unless the service provider can prove that it acted in accordance with the Minister's notification regarding notice procedure, suspension of dissemination of compute data and removal of such computer data.

Under Section 16/2, once the service provider is aware that electronic data in its possession is the data ordered for destruction by the court order, it must destroy the data. If it fails to do so, the service provider shall be subject to half of the penalty as provided for the relevant offence.

4. NATIONAL SECURITY AND EMERGENCY POWERS

The legislation provided above describes Thai law in ordinary times. Thailand is currently under the de facto control of a military junta. As a result, NCPO Order No. 3/2558 (3/2015) re: Maintaining Public Order and National Security issued by the Head of the National Council for Peace and Order (the "NCPO") under Section 44 of the Interim Constitution and the Interim Constitution 2014 (both described below) currently supersedes the legislation described above.

4.1 Constitution of the Kingdom of Thailand (Interim) B.E. 2557 (2014) (the "Interim Constitution")

Section 44 of the Interim Constitution provides the NCPO with wide powers to take any extrajudicial action it deems necessary against any act which undermines public peace and order or national security. Under section 44, it may suspend or take action, regardless of its effect on the legislative or executive arms of the government or the judiciary, in situations where it is necessary for benefit or reform in any field and to strengthen public unity and harmony, or for the prevention, disruption or suppression of any act which undermines public peace and order, national security, the monarchy, national economics or the administration of state affairs.

4.2 NCPO Order No. 3/2558 (2015) Re: Maintaining Public Order and National Security ("Order No. 3/2558")

Following the termination of martial law on 1 April 2015, the NCPO issued NCPO Order No. 3/2558 under Section 44 of the Interim Constitution. This implements measures to deal with actions intended to undermine or destroy peace and national security, violate notifications or orders issued by the NCPO.

NCPO Order No. 3/2558 deals primarily with the maintenance of public order and national security. In particular it gives extensive legal powers to certain categories of military officers that it refers to as "Peacekeeping Officers". The breadth of its provisions and the exact manner in which such provisions may be exercised remains unclear.

NCPO Order No.3/2558 provides Peacekeeping Officers with broad legal authority to prevent and suppress offences related to (i) lèse majesté; (ii) internal security of the Kingdom; (iii) the laws on firearms; and (iv) any violation of any other orders issued by the NCPO. The order also empowers Peacekeeping Officers to issue orders prohibiting the propagation of any item of news or the sale or distribution of any book or publication or any material likely to cause public alarm to the detriment of national security or public order.

Any actions done by Peacekeeping Officers in good faith, without discrimination, in a proportionate manner, and without undue severity, shall not be subject to judicial review, either by an administrative court, civil court, or criminal court.

On April 16, 2015, NCPO Order No. 5/2558 (2015) was issued to amend Order No. 3/2558. Its provisions can be summarised as enabling additional categories and ranks of military officer to become Peacekeeping Officers.

4.3 Martial Law Act B.E. 2457 (1914) (the "MLA")

Following the imposition of martial law on Thailand in 20 May 2014, the NCPO were vested with extensive powers of government. While martial law has been revoked under Order 3/2558, it remains in force in Thailand's southern border provinces of Pattani, Yala, Narathiwat and Songkhla. In relation to surveillance and censorship of communications data specifically, the following provisions may provide the NCPO with wide powers. However, the exact manner in which such provisions may be exercised remains unclear.

Under section 10, the military authority may require from any person or company any conveyance, beast of burden, provisions, arms, instruments and tools for use in military service at that time.

Section 12 states that the military authority may, if it deems appropriate, cause provisional seizure of all things so as to prevent the enemy from using them or for the benefit of military service.

The below legislation also provides for special powers in times of national security or emergencies.

4.4 Internal Security Act B.E. 2551 (2008) (the "Internal Security Act")

Under the Internal Security Act, arrests and prosecutions must follow legal procedures. However, the definition of "threat" under the Internal Security Act is vague, and the NCPO therefore have wide discretion to determine what is and is not a "threat" and what activities to monitor. It gives officials of the Internal Security Operations Command (a unit of the Thai military dedicated to national security issues) a wide range of police powers normally exercised by civilian authorities, including powers to use both lethal and non-lethal force, to

arrest and detain individuals, to conduct searches, to enter premises overtly and covertly, and to bring criminal charges.

4.5 Telecommunications Business Act B.E. 2544 (2001) (the "TBA")

Under section 63 TBA, the National Broadcasting and Telecommunications Commission is given wide powers in the event of an emergency, or where necessary to maintain public order, national security or economic stability or to protect public interests. It may take possession of and use the devices and equipment of the licensed telecommunications provider, or authorise a state agency to temporarily take charge of a telecommunications provider's services, or order the telecommunications business or his/her employees to take a specific action until the end of such emergency or necessity.

4.6 Radio Communications Act B.E. 2544 (2001) (the "RCA")

Under section 14 RCA, for the purpose of maintaining the public order or defending the realm, the Minister of MDE is empowered to issue a provisional order to the competent authority to seize, put to use, prohibit the use of, or prohibit the removal of radio communication equipment, or part thereof, within the period and under the conditions specified in the order.

4.7 NCPO notification no. 26/2557 (2014) on supervision and surveillance on the use of online social media (the "NCPO Notification No. 26/2557")

NCPO Notification No. 26/2557 was issued on 24 May 2557 (2014). Under this notification, the permanent secretary of the ICT ministry shall establish an online social media committee which has the power to examine, inspect, and access "online information". It has broad powers to suspend or close online publications, websites and social media platforms on a number of grounds, including for engaging in incitement of hostility or agitation, for undermining the credibility or integrity of the law, or resisting or opposing the performance of the NCPO's duties. The notification does not provide any guidance as to how such powers shall be exercised by the committee.

Please note that since the abolition of martial law, the Peacekeeping Officers under Section 4(4) of Order No. 3/2558 are empowered to police any violations of this Notification.

5. OVERSIGHT OF THE USE OF POWERS

At the time of this report, Thailand is under an indefinite state of emergency and thus the applicable oversight functions set out below may not be followed.

The expansive powers given to the authorities by the Internal Security Act, the Martial Law Act, and the NCPO Order No. 3/2558 (2015) are subject to almost no independent oversight mechanisms (save for the fact that actions which are not in good faith, discriminatory or disproportionate could be subject to judicial review). The Prime Minister is required, under the Internal Security Act, to report to the parliament when the 'threat to internal security' has subsided or can be addressed within the normal powers of the government agencies.

5.1 Administrative Court Procedure Act B.E. 2542 (the "ACP")

Decisions of the National Broadcasting and Telecommunications Commission can be appealed within the organisation itself, but may also be appealed to the ACP.

An administrative case is generally initiated in the Administrative Court of First Instance, unless provisions of a specific act specifically state the dispute be filed directly at the Supreme Administrative Court.

When a dispute is to be filed at the Administrative Court, the procedure follows an inquisitorial system and any decision made by the Administrative Courts of First Instance may be appealed to the Supreme Administrative Court.

6. PUBLICATION OF AGGREGATE DATA RELATING TO USE OF GOVERNMENT POWERS

Restrictions on network operators and service providers

Ordinarily there is no legislation which prevents the publication of aggregate data relating to the use by the government of the powers described in this report. However under the expansive extrajudicial powers vested in the government under NCPO Order No. 3/2558 issued under Section 44 of the Interim Constitution, it has the authority to restrict publishing of any types of data which are not in the national interest.

Aggregate data published by government agencies

As far as we are aware, the government does not publish aggregate data relating to its use of the powers described in this report.

7. CYBERSECURITY

Thailand is yet to directly legislate on cybersecurity measures that must be taken by business operators of electronic communications networks and services to protect their data from cybersecurity threats or attacks.

However, cybersecurity requirements have been stipulated under the Electronics Transaction Act B.E. 2544 (2001) which regulates many different types of electronic transactions. There are also cybersecurity requirements contained within sector-specific statutes such as the Telecommunications Business Act B.E. 2544 (2001), the Financial Institution Business Act B.E.2551 (2008), and the Securities and Exchange Act B.E. 2535 (1992). A discussion of some of these provisions, along with others, follows below.

7.1 The Telecommunications Business Act B.E. 2544 (the "TBA")

Under Section 50 TBA, the National Telecommunications Commission (the "NTC") has the authority to prescribe measures for consumer protection purposes on matters pertaining to personal data, rights of privacy and the freedom to communicate. By the power vested to it under the TBA, the NTC has issued the "Notification of the NTC re: procedure for

protection of data privacy and rights of telecommunications" (the "Notification") on 16 August 2006 which prescribes standard measures that telecommunication service providers must adhere to.

Pursuant to Section 10 of the Notification, telecommunication service providers are under an obligation to establish appropriate data protection measures and improve such measures from time to time in accordance with the advancement of technology. If a licensed telecommunication service provider fails to comply with this security requirement, the Secretary-General of the NTC may issue a written warning to the licensed service provider demanding that they comply with the requirements. In the event that the licensed service provider continues to fail to comply with the outlined requirements, the Secretary-General of the NTC has the power to impose an administrative fine not less than twenty thousand Baht per day that the failure to comply continues or a suspension order under Section 64 TBA. Should the licensed service provider further ignore their obligations to establish and improve appropriate data protection measures, violate the license suspension order, or cause serious damage which is of public interest, the NTC pursuant to Section 66 TBA has the power to further suspend and even revoke the service provider's telecommunication licence.

Furthermore, under Section 61 TBA, a competent official may enter a building or operating site of a telecommunication licensee during the period between sunrise and sunset, or during the business hours of such a place for the purposes of inspection of the business's operation, books of account, documents or related information in relation to any action that may violate the provision of the TBA (which may include the failure to comply with a specified provision of the licence). Failure to comply with an order of a competent official could lead to a fine of up to 10,000 Thai Baht and/or imprisonment for up to one month.

Under Section 63 TBA, in cases of a public emergency or where it becomes necessary to maintain public order, national security or economic stability or to protect the public interest, the NTC has the authority to take possession of and use the devices and equipment of licensed telecommunications businesses. The NTC may alternatively authorize a state agency to temporarily take possession of such equipment or order a telecommunications business or his/her employees to take certain action until the end of the emergency or necessity. Failure to comply with such an order could lead to a fine of up to 100,000 Thai Baht and/or imprisonment of up to six months.

The criminal penalties that may apply where a breach of the TBA is discovered (not including administrative penalties) can be extended to the directors or managers responsible for the service provider in question.

Also note that under Section 50, in circumstances where there has been a violation of a user's data privacy rights, a licensed service provider is required to take action to terminate such violation and inform the user without delay.

The TBA generally serves to protect telecommunication providers from third party access, interception and disclosure. It does however, as stipulated above, provide for an extension of executive power in the way that it allows government authorities, particularly where communications have national security implications, concern the public order or the good morals of Thailand, to take possession of a licensed telecommunications business's equipment, order an agency to take such possession or order that the licensed telecommunications business themselves take action that the government authorities require.

Under Section 65 TBA, where a licensed telecommunication service provider is not satisfied with an order of the Secretary-General of NTC regarding the suspension or revocation of their licence or the manner in which any other administrative has been exercised under Section 64 TBA, the licensed service provider has the right to appeal to the NTC within fifteen days from the date of receiving the written order they are aggrieved by. The decision of the NTC on the appeal shall be final. To appeal this second level decision of the NTC, the licensed service provider would be required to initiate legal action in the Administrative Courts under Section 44 of the Act on Establishment of Administrative Courts.

7.2 Electronic Transaction Act B.E. 2544 (2001) (the"ETA")

The ETA is the primary legislation governing all commercial transactions performed using electronic means in Thailand. The ETA was introduced with the purpose of creating an adequate regulatory environment to ensure and promote the reliability of electronic transactions in Thailand. As such, the ETA also contains cybersecurity requirements which relate to the use of electronic transactions.

7.2.1 Royal Decree Regulating Electronic Payment Service Business B.E. 2551 (2008) ("E- Payment Law").

The E-Payment Law was issued under the ETA by the Bank of Thailand to regulate select electronic-payment businesses. Under the E-Payment Law, these select electronic payment services are categorized into either List A, List B, or List C, all of which shall be subject to the prior notification of, registration with or license from the Electronic Transaction Committee ("ETC").

The regulated payment services covered by the three lists discussed above (A, B and C) include:

- E-money Services;
- Credit Card Network Services;
- EDC Network Services;
- Transaction Switching Services for payment;
- Clearing Services;
- Settlement Services;
- Electronic Payment Services through any device or

network; and

- Payment Collection Services.

Under Section 10 of the E-Payment Law, the regulated service provider is required to submit to the ETC a contingency plan or a back-up system if faced with a failure of their system to ensure that they can continuously provide the e-payment service. This includes a requirement that their information technology systems maintain a security standard not less than the standard prescribed by the Bank of Thailand. Additionally, regulated service providers under the E-Payment Law are required to examine and maintain the security of their system for consistent reliability under Section 16(2) E-Payment Law.

If the service provider violates or fails to comply with the cybersecurity requirements of the E-Payment Law, the ETC holds the power under Section 34 to impose an administrative fine not exceeding two million Thai Baht. Furthermore, should a regulated service provider fail to comply with an order of the ETC, the ETC has the power again under Section 34 to suspend or revoke the e-payment license.

7.2.2 The Royal Decree on Security Procedure for Electronic Transaction B.E. 2553 (2010) (the "RDSPET")

The RDSPET imposes cybersecurity requirements on certain types of businesses that are deemed to carry out sensitive activities related to national security and critical public infrastructures. The RDSPET sets out the varying types of security and safety into three different levels; (i) standard security, (ii) normal security and (iii) strict security. The level of security that will apply to the types of businesses that fall under the RDSPET will depend upon the business's sensitivity to threats.

Under Section 2 (6) of the "Notification of Electronic Transaction Committee re category of electronic transactions and rules on assessment on the scale of impact of electronic transactions" pursuant to "Security Techniques B.E. 2555 (2012)" which was issued under the RDSPET, e-payment businesses and businesses relating to public infrastructure that are required to be used continually (i.e. without interruption) or in an on-going manner shall be subject to strict security requirements. Other businesses which also fall under this category are banking, insurance and securities related businesses. It is also likely that a telecommunication business will be deemed a business that provides public infrastructure which is required to be used continually without interruption. However, there is no legislation or case law to date that confirms the ETC would treat a telecommunications company as falling within this category.

Where a business is deemed by the ETC to fall within the category of businesses to which the strict security requirements outlined by the RDSPET would apply, they would additionally be required to implement the standard of IT security measures outlined within the Notification of Electronic Transaction Committee re: Standards of IT Security Procedure B.E. 2555 (2012). These IT security measures include:

- the management of all security measures put in place to prevent the unauthorized access of the collected data;
- the maintenance of their information security; and
- the capability of their system to continually provide the service in question.

There are no specific administrative or criminal penalties provided under the RDSPET or the ETA where non-compliance with the RDSPET is discovered. The ETA simply provides that if an operator had complied with the above regulations, their business operation will be assumed under Section 25 ETA to provide reliable electronic transactions.

The agencies responsible for the administration of the ETA include the Ministry of Digital, Economic and Society (the "MDE"), the ETC and the Bank of Thailand in the case of the E-Payment Law.

7.3 Data Protection Draft Bill

The Data Protection Law is currently in the legislation process as a draft bill and is currently under the consideration of the MDE. It remains unclear at this stage when the law will be passed to the National Legislative Assembly and therefore when it will come into effect.

However, it is worth noting that under Section 29 of the draft law, specific requirements of data managers are provided for. These include putting in place appropriate measures to ensure the security of their data privacy and destroying the privacy data after the end of storage period or the consent has been withdrawn.

A manager also under Section 29(4) has a legal duty to notify any user affected of any violation suffered to its private data. If the amount of such users is over the limit specified by the Privacy Protection Committee, the data managers shall promptly notify the Privacy Protection Committee and provide them with details of the measures taken to remedy the data breach.

A data manager who fails to comply with the above requirement is subject to a penalty of imprisonment up to six months and/or a fine not exceeding five hundred thousand Thai Baht.

8. CYBERCRIME

8.1 Computer Crime Act No. 2 B.E. 2560 (2017) (the "CCA")

The CCA was published on the Royal Thai Government Gazette on 24 January 2017 and shall therefore become effective within 120 days from the publication. It acts as the primary legislation governing cybercrime in Thailand and address criminal acts such as hacking, the disclosure of passwords, eavesdropping on computer data, pornography and other "harmful" internet content and stipulates the liability of internet service providers when such crimes are discovered. The CCA also gives competent governmental officials the power to restrict the dissemination of computer data or websites. Violations of the CCA are punishable in the following ways:

Statutory Reference	Offence	Penalty
Sections 5 and 12	Hacking Described as illegally accessing or eavesdropping on a computer system or data for which a specific access prevention measure that is not intended for their own use is available or disclosure of the method of doing so.	Imprisonment for no longer than 6 months or a fine of not more than 10,000 baht or both. If such offense is committed against computer data or computer systems in relation to national security, public safety, national economic stability, or public infrastructure there is a mandatory sentence of imprisonment of 1 to 7 years and a fine of 20,000 to 140,000 baht. If such offense mentioned in the above paragraph causes damage to such computer data or computer system there is a mandatory sentence of imprisonment of 1 to 10 years and a fine of 20,000 to 200,000 baht.
Section 9, 10, 12, and 12/1	Damaging a Computer System or Data Described as illegally damaging, destroying, correcting, changing or amending a third party's computer data or committing any action to suspend, delay, hinder or disrupt a computer system to the extent that the computer system fails to operate normally.	Imprisonment for no longer than 5 years and/or a fine of not more than 100,000 baht. If such offense is committed against computer data or computer system in relation to national security, public safety, national economic stability, or public infrastructure there is a mandatory sentence of imprisonment of 3 to 5 years and a fine of 60,000 to 300,000 baht. If such offense causes harm to other person or their property, there is a mandatory sentence of imprisonment for not more than 10 years and a maximum fine of 200,000 baht. If such offense is committed unintentionally but causes the death of a person, the offender shall be subject to imprisonment for 5 to 20 years and a fine of 100,000 to 400,000 baht.

Statutory Reference	Offence	Penalty
Sections 5 and 12	Hacking Described as illegally accessing or eavesdropping on a computer system or data for which a specific access prevention measure that is not intended for their own use is available or disclosure of the method of doing so.	Imprisonment for no longer than 6 months or a fine of not more than 10,000 baht or both. If such offense is committed against computer data or computer systems in relation to national security, public safety, national economic stability, or public infrastructure there is a mandatory sentence of imprisonment of 1 to 7 years and a fine of 20,000 to 140,000 baht. If such offense mentioned in the above paragraph causes damage to such computer data or computer system there is a mandatory sentence of imprisonment of 1 to 10 years and a fine of 20,000 to 200,000 baht.
Section 11 and 12	Spamming Described as sending computer data or electronic mail to another person and covering up the source of the sender in a manner that disturbs the other person's normal operation of their computer system or leaves them without an option to deny the reception.	A fine not exceeding 100,000 baht. If such offense is committed against computer data or computer system in relation to national security, public safety, national economic stability, or public infrastructure there is a mandatory sentence of imprisonment for 1 to 7 years and a fine of 20,000 to 140,000 baht. If such offense mentioned in the above paragraph causes damage to such computer data or computer system there is a mandatory sentence of imprisonment for 1 to 10 years and a fine of 20,000 to 200,000 baht.
Section 14	Putting or Spreading Illegal Data into a Computer System Described as putting pornography, faulty data, or pictures of another person on a computer system in a manner that is likely to cause damage to their reputation, public security, national security, national economic security or public infrastructure serving the public interest or cause panic in the public.	Imprisonment up to 5 years and/or a fine not exceeding 100,000 baht (A service provider who cooperates, consents or acquiesces with an offender to the commission of this crime is subject to the same penalty imposed upon the person committing the offence pursuant to Section 14 and 15 CCA).
Section 16/2	Keeping of Illegal Material or Data Described as maintaining possession of computer data which is ordered for seizure and destruction by the court.	16 of CCA.

8.2 Telecommunications Business Act B.E. 2544 (the "TBA")

The National Telecommunications Commission (the "NTC") has the authority to punish breaches of the TBA in the following ways:

Statutory Reference	Offence	Penalty
Section 74	Illegally intercepting, utilising or disclosing news or a message or any other information communicated via telecommunications.	Imprisonment for no more than 2 years and/or a fine of not more than 400,000 Thai Baht. The said penalty (not including administrative penalties) could extend to the directors or managers responsible for the service provider in breach.

8.3 Act on Organization to Assign Radio Frequency and to Regulate the Broadcasting and Telecommunications Services B.E. 2553 (2010) (the "AOARF")

Under Section 32 AOARF, where the above crime is committed (i.e. where the illegal interception, utilization or disclosure of a message, information or any other data by means of telecommunications is discovered), it is the Telecommunications Commission (the "NBTC") who is to be considered as the individual affected and damaged under the Criminal Procedure Code. In line with this, the NBTC holds the following powers:

Statutory Reference	Offence	Penalty
Section 32	Where a telecommunications service provider is the offender in question or knows that an offence has been committed but refrains from taking notice or action in accordance with the law within a reasonable amount of time.	Suspension or revocation of the provider's telecommunications business license.
Section 77	Where a broadcasting or telecommunications business operator fails to comply with an order of the NBTC.	An administrative fine not exceeding five million Baht and a fine not exceeding one hundred thousand Baht per day that the order is not observed.

8.4 Radio Communication Act B.E. 2498 (1955) (the "RCA")

The Radio Communication Act governs signal transmission activity, including radio, signal, wave and broadcast

Statutory Reference	Offence	Penalty
Section 16 and Section 23	Transmitting a communication through radio signals of any message known to be false which may cause damage to the nation or to the public.	Imprisonment of no more than five years and/or a fine of not more than THB 100,000.
Section 17 and Section 25	Intercepting for use or unlawfully disclosing radio communication news which is not for the purpose of public benefit or may cause public damage.	Imprisonment of no more than 2 years and/or a fine of not more than THB 40,000.

Under Section 14, for the purpose of maintaining public order or protection of the nation, the Minister of MDE has the right to issue a provisional order to seize for use, restrict use, or restrict the movement of radio communication devices.

8.5 National Cybercrime Draft Bill

As discussed above, a specific law governing cybercrime in Thailand, the National Cyber Crime Draft Bill, is currently under the review by the Office of the Council of State. Upon completion of the review, the Office of Council of State will submit the reviewed draft for the cabinet's approval and the cabinet will submit the draft for National Legislative Assembly's examination. It is therefore unclear at this stage when the draft bill will be finalized and come into effect.

Note, however, that under the current draft, Section 6 proposes to establish a National Cybersecurity Committee which will be tasked with detecting and countering online threats to national security, stability, the military and economy.

Moreover, under Section 35(3) of the current draft, the National Cybercrime Committee has relatively broad powers for the purpose of fulfilling its cybersecurity duties in relation to national interests which include accessing the personal information in and intercepting the communication from any electronic devices without requiring a court order.

Under the CCA, there are numerous illustrations of an extension of executive powers when cybersecurity breaches are discovered. For example:

- under Sections 18(1), (2), and (3), competent officers of the MDE are empowered to send enquiry letters, summon concerned persons for interrogation and request statements, documents, computer data, computer traffic data and other evidence from service providers without a court order;
- with a court order, officers of the MDE may order an internet or telecommunication service provider to copy or hand over certain data pertaining to users, (that data service providers are obligated to keep under the law) and potentially compel service providers to assist with decrypting encoded data under Sections 18(4)-(8); and
- under Section 20(3) (which was recently amended), where content is considered to be against public order or good morals of the public, the content may be banned and ordered to be deleted pursuant to a court order, based on a request from a Computer Data Screening Committee, who were appointed by the Minister of Digital Economy and Society to make decisions concerning whether content consists of illegal information.

With regard to the extension of executive powers provided for by the TBA and RCA, see the relevant paragraphs of the 'Cybersecurity' section above.

A non-Thai citizen engaging in criminal activities may be subject to the CCA. Section 17 CCA stipulates that the person committing the offence under the CCA outside of the Kingdom of Thailand shall be penalized within Thailand if the offender is a Thai citizen or the offender is a non-citizen but the Thai government or a Thai person is an injured party.

With respect to other related laws, the general rule on territory under the Criminal Code shall apply.

An alleged offender charged with one of the cybercrimes stipulated above has the right to appeal to the Appeal Court or Dika Court (i.e. the Supreme Court) under the Criminal Procedure Code.

Law stated as at 22 February 2017.