telenor group

AUTHORITY REQUESTS FOR ACCESS TO ELECTRONIC COMMUNICATION – legal overview

MARCH 2017

CONTENTS

INTRODUCTION

INTRODUCTION

Following our legal overview report relating to lawful access to communications, first published in May 2015, this document provides an updated overview of the most common kinds of laws which compel the Telenor Group to give government authorities access to customer communications in 13 of the countries in which Telenor operates. As well as refreshing each country report in relation to any changes to the relevant legislation since 2015, we have also added entirely new sections relating to cybersecurity and to cybercrime.

Whilst the laws themselves are all publicly available, in practice they tend to be little known and not well understood by the public. By publishing this document Telenor aims to increase transparency in this space to its customers and other stakeholders.

These laws include those that compel us either to divulge information about our customers and their communications to certain government authorities, typically secret intelligence services and law enforcement agencies, or to prevent or suspend access to certain content or services.

These types of laws are primarily devised to investigate or prevent crime and terrorism, and to safeguard national security and public safety. The government bodies that use these laws to obtain information from telecommunications network operators and service providers such as Telenor assert that such information is vital to the performance of their duties.

THE DIFFICULTY OF REPORTING ON THE LAWS

Compiling a summary report of the most commonly used laws giving government authorities access to customer communications for each of Telenor's markets has been a difficult and challenging task.

The detail and scope of the laws in question varies greatly between the different countries in which Telenor operates, reflecting our presence in Europe and in Asia. The laws themselves are all too often opaque and poorly written. As such, they can be hard to interpret, even for legal specialists.

In many countries the laws were originally conceived in the late nineteenth or early twentieth centuries to allow police or intelligence agencies to intercept and read letters and telegraphs, and place wiretaps on telephone landlines. Concepts and terminology appropriate for this earlier era do not easily fit into the context of today's world of smartphones, the internet and social media.

There is a notable lack of consistency in even the most fundamental legal terms and concepts. Some governments have constrained powers that limit the impact on an individual's rights to privacy and freedom of expression; others use much wider-ranging powers with substantially greater human rights impacts. Some of the statutes in question are lengthy and contain carefully expressed checks and balances. Others are only a few pages long, with unchecked and sweeping powers set out in a few short sentences.

In this document, we provide a country-by-country insight into the nature of the local legal regime governing law enforcement assistance.

OUTLINE OF THE TYPES OF LAW FEATURED IN THE REPORT

Lawful Interception

Most countries have laws that enable government authorities to order companies that provide communication services and/or operate telecommunications networks (CSPs) to allow the interception of their customers' communications. For example, to listen to a phone call, or to read an email. In practice, this means that the CSPs have to configure their own systems to give one or more government agencies real time access to the contents of communications.

The nature of the access that the CSP is obliged to give to its own network can vary greatly from one country to another. As the most intrusive form of government access, it is common for interception to be lawful only if a warrant has been issued for it and presented to the CSP in question. In some countries, limited access is granted on a case by case basis following the issuing of such a warrant by a court or public prosecutor. In others, the CSP must allow permanent direct access to its network with no control or visibility over the interception activities that the government in question carries out.

Frequently, the legislation does not explicitly state how authorised interceptions may be carried out in practice and such information is often confidential. However, we have sought to clarify the nature of law enforcement agencies' access to communications in each country, where possible.

DISCLOSURE OF COMMUNICATIONS DATA

Every communication over a telecommunications network automatically generates certain kinds of technical data within the network itself. This metadata, at its simplest, is the information that the network needs in order to route the communication between sender and recipient.

We shall refer to such metadata as "communications data" in this report. It is often described as the 'who, where, when and how' of a communication. Importantly, it does not include the content of a communication. Communication includes the sending of data between computer servers, so communications data would include the IP address assigned to a device making or receiving a communication.

Because an analysis of communications data can reveal a

large amount about an individual's movements and their social and professional relationships, it is regarded as an extremely useful resource for government agencies undertaking any form of investigation. Coupled with the fact that the disclosure of communications data has traditionally been regarded as less of an invasion of privacy than intercepting a communication, almost all countries have laws that enable government agencies to require CSPs to disclose significant amounts of communications data to them.

As with interceptions, the forms that such disclosure can take and the degree of legal scrutiny or other oversight surrounding it vary greatly from country to country. In some legal jurisdictions, a government agency may have direct access to any communications data that it wants. However, it is more common to find some degree of legal process or oversight, though a warrant may not necessarily be required to accompany each disclosure request. Many countries also allow access to communications data in 'threat to life' scenarios, for example where a person has gone missing and the geo-location data of their mobile phone may indicate their location.

NATIONAL SECURITY

Safeguarding national security is a fundamental duty of every government. As such, those government agencies charged with protecting and investigating threats to national security tend to be given greater legal powers than those given to law enforcement bodies. This is particularly true in relation to legal powers relating to interception and to disclosure of communications data, where intelligence agencies tend to be given a greater degree of discretion than law enforcement agencies.

In many countries, the definition of what constitutes a threat to national security is set out in detail in legislation dedicated to national security or intelligence matters. This specificity helps circumscribe the powers of, for example, the domestic intelligence services. In other countries, the scope of national security powers is wider. This often means that the distinction between the powers that law enforcement bodies have to access data to investigate crimes, and the powers that intelligence agencies have to investigate threats to national security, is less clear.

EMERGENCY OR CRISIS POWERS

Many countries have legislation that gives extraordinary legal authority to the government during periods of national emergency or crisis. These types of laws are typically drafted with natural disasters, wars and widespread civil disorder in mind. The laws generally enable government agencies to assume direct control of certain essential national infrastructure for the duration of the emergency, including telecommunication networks.

In some countries, the legislation names the CSPs whose networks may be taken over. In others, the government can choose to take control of any CSP's network. Emergency legislation of this type tends to be (but is not always) tightly controlled, for example requiring parliamentary approval for its use.

Powers to restrict web browsing or order network or service shut-down

This report also identifies legislation which allows governments to block a CSP's network or services. These tend to be laws that either restrict the CSP from allowing users to access certain kinds of online content or that allow the government to shut down the CSP's entire network or (more commonly) particular services (for example, temporarily suspending a mobile phone network or an instant messaging service in a particular city during a riot).

In terms of IP address blocking, many countries have laws that enable government authorities to order CSPs to prevent access to certain kinds of illegal or offensive content by anyone using their network. Typically, the scope of what constitutes illegal content is limited in the relevant legislation either to that depicting criminal offences such as child abuse or murder, or to websites offering activities that are illegal in the country in question (a common example is online gambling). The laws generally include the ability of the government to maintain an updated list of certain IP addresses and websites that must be blocked.

In other countries, illegal content is defined more broadly. Sometimes the definition of illegal content includes websites offering commentary that, for example, is critical of the government or of particular religious or ethnic sensitivities. In such cases the legislation, in effect, gives the government the power to censor public discussion of certain subjects.

In terms of the laws that enable shut down or suspension of a CSP's network or particular service, these are typically drafted to assist law enforcement agencies in tackling civil disorder, such as riots.

NEW SECTION – CYBERSECURITY AND CYBERCRIME

This updated report now also includes details of the laws in each country which relate to the linked topics of cybersecurity and cybercrime.

Cybercrime comes in many shapes and sizes, but generally relates to some form of unauthorised interference with a software application and/or computer server (including systems, network infrastructure and data), commonly referred to as 'hacking'. Examples of cybercrime include unauthorised access to information in computer systems, knowingly sending computer viruses or conducting distributed denial of service (DDoS) attacks. In some cases countries apply existing criminal law to these kinds of activities. However, as the scale and sophistication of cybercrime has developed in recent years, many countries have introduced specific legislation that identifies such activities as criminal offences and brings a range of penalties to bear on those responsible.

Many countries have also introduced legislation containing obligations in relation to cybersecurity. Such laws generally require companies operating in specific sectors (including communications service providers) to take prescribed measures to protect themselves and their customers against cybercrime. Typically there is a focus on the resilience of services considered critical to the functioning of society, for

example on water or electricity suppliers. The measures may include requirements to meet specified information security standards, to report data breaches or hacking incidents to regulators and to customers whose data is affected. Failure to comply with these requirements often results in substantial fines for the offending company.

Some countries have adopted a similar approach to the upcoming European Directive 2016/1148 on the security of network and information systems (NIS Directive) by establishing computer security incident response teams ("CSIRTs") which monitor compliance with cybersecurity standards and coordinate the reaction and response to cybersecurity crises.

As these are still emerging issues, some countries have naturally progressed further than others in their efforts to legislate. However, it is likely to be an area in which will see increasing regulation. This report gives a summary of the relevant legislation in each country at the date of publication.

BANGLADESH – 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 law of the People's Republic of Bangladesh.

1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

1.1 Bangladesh Telecommunication Regulatory Act, 2001 (the "BTRA")

Section 35 BTRA requires every person establishing or operating a telecommunication system to have a licence. The term, "person" is defined in section 2(24) of the BTRA and includes any natural person, partnership, society, company, corporation, co-operative society or statutory body. In addition, the definitions of "telecommunication", "telecommunication system" and "telecom service" are widely drawn, covering users and service providers in connection with telecommunication services and apparatus.

Section 97(Ka) BTRA (as introduced by the Bangladesh Telecommunications (Amendment) Act 2006) is the sole statutory basis from which the government derives its powers in relation to surveillance and censorship, as outlined below.

Under section 97(Ka) BTRA, on the grounds of national security and public order, the government may empower certain government authorities (intelligence agencies, national security agencies, investigation agencies, or any officer of any law enforcement agency) to suspend or prohibit the transmission of any data or any voice call, and record or collect user information relating to any subscriber to a telecommunications service. This widely drafted provision encompasses interception capabilities. The relevant telecoms operator must provide full support to the authority empowered to use such powers. The BTRA does not provide for any time limits on these powers. As a result, an interception may last for as long as the agency implementing the interception decides.

Under this section, "government" means the Ministry of Home Affairs; provisions under this section are applicable upon approval by the Minister or State Minister of that Ministry.

1.2 Information and Communication Technology Act 2006 (the "ICT Act")

The ICT Act regulates the use of digital signature certificates and the provision of data services and defines a series of offences related to malicious activity online. It provides remedies for offences such as unauthorized damage to computer systems, tampering with computer source code, hacking, publishing false, obscene or defamatory information in electronic form, and publishing false digital signature certificates.

The ICT Controller is an officer appointed under the ICT Act and regulates its implementation. Under section 29 of the ICT Act, the Controller, or any officer authorised by him should investigate any contravention of the ICT Act, or the rules or regulations made under it. In order to do so, the Controller or authorised officer has the same powers as those vested in a Civil Court under Bangladesh's Code of Civil Procedure, which include powers of "discovery and inspection" and "compelling the production of any document".

Under section 30, the ICT Controller may access any computer system, apparatus, data or other material connected with a computer system for the purpose of searching or causing a search to be made for obtaining any information contained in or available to the computer system. The ICT Controller may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

Under section 46 of the ICT Act, if the ICT Controller feels that, in the interests of the sovereignty, integrity, or security of Bangladesh, international relations, public order or for preventing incitement to commission of a legally recognised offence, it is necessary or expedient, they can direct any law enforcement agency of the government to intercept any information transmitted through any computer resource. In

addition, they may order the subscriber or any person in charge of a computer resource to provide all necessary assistance to decrypt the relevant information. The reasons for undertaking such a measure must be recorded in writing.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Bangladesh Telecommunication Regulatory Act, 2001 (the "BTRA")

There is no direct reference in the BTRA to storage of metadata. In general, storage of data relating to customers is likely to be a condition of a telecommunication operator's individual licence, which commonly requires operators to store metadata for a specified period of time. As billing is done on a monthly basis, operators need to store metadata for subscribers at least for a sufficient period so that the subscribers may make enquiries or seek an itemised bill before payment.

Under the broad powers granted in section 97(Ka) BTRA, on the grounds of national security and public order, the government may require a telecommunications operator to keep records relating to the communications of a specific user. However, when considering whether to make a retention request, the relevant government agency would need to consider the technical resources and capabilities of the operator to retain information.

2.2 Information and Communication Technology Act 2006 (the "ICT Act")

The ICT Controller or any person authorised by him can seek metadata when exercising the investigatory powers provided under section 29 of the ICT Act for the purpose of discovery and inspection, enforcing the attendance of any person and examining him under oath or affirmation, compelling the production of any document, and issuing commissions for the examination of witness for any offence committed under the ICT Act.

3. NATIONAL SECURITY AND EMERGENCY POWERS

3.1 Bangladesh Telecommunication Regulatory Act, 2001 (the "BTRA")

Under section 96 BTRA, the government may, on the grounds of public interest, take possession of any telecommunication system, and any arrangements that are necessary for operating it. It may continue such possession for any time period and keep the operator and his employees engaged on a full-time basis or for a particular time for the purpose of operating such apparatus or system. The government is obliged, however, to pay proper compensation to the owner or the person having control of the radio apparatus or the telecommunication system over which it takes control.

Under section 97 BTRA, when a foreign power declares a state of war, or creates a warlike situation against Bangladesh, when there is an internal rebellion or disorder, or in a situation where the defence or security of Bangladesh or any other urgent state-affair needs to be ensured, the government will have priority over the operator or any other user regarding the use of a telecommunication system.

Moreover, if the President of Bangladesh declares a state of emergency, the government may suspend or amend any licence or certificate or permit issued under the BTRA, or suspend any particular activity of, or a particular service provided by, an operator.

Section 97(Ka) BTRA, as outlined in the sections above, is also applicable in states of emergency or national security.

Furthermore, section 66(Ka) BTRA (incorporated by the Bangladesh Telecommunications (Amendment) Act 2006) empowers the Bangladesh Telecom Regulatory Commission (the "BTRC") to stop any signal, message or request from any subscriber (where it is expedient to do so), in the interest of the sovereignty, integrity, or security of Bangladesh, international relations, public order or for preventing incitement of a legally recognised offence. Operators must assist the BTRC to implement this order.

3.2 Telegraph Act 1885 (the "1885 Act")

It should be noted that some relevant sections of the BTRA's predecessor, the Telegraph Act 1885 (the "1885 Act") are also still in force. However, no operating licences are currently issued under the 1885 Act. As a result the following provisions are no longer used, though we mention them for the sake of completeness:

- Section 5 of the 1885 Act provides that, in the case of a public emergency or in the interest of public safety, the government or any officer authorised by the government, may take temporary possession of any telegraph established, maintained or worked by any person licensed under this Act.
- Under the 1885 Act the government or are authorised officer may order that any message or class of messages to or from any person or class of persons (relating to any particular subject) sent or received by any telegraph, may be blocked, intercepted or detained by, or disclosed to, the government or an officer thereof mentioned in the order.

4. CENSORSHIP

4.1 Bangladesh Telecommunication Regulatory Act, 2001 (the "BTRA")

It should be noted that the national security-related powers granted under s. 97(Ka) BTRA discussed above in section 3.1 could, at least in theory, be used for the purposes of censorship.

4.2 Information and Communication Technology Act 2006 (the "ICT Act")

Under section 45, the ICT Controller (explained above) may issue an order to a licence-holder under the ICT Act to take certain measures or cease certain activities as specified in such order, if necessary to ensure compliance with the provisions of the ICT Act, or rules and regulations made under it.

Under sections 57 and 59 of the ICT Act, if any person deliberately publishes or transmits, or causes to be published or transmitted, on a website or in any electronic form any material which:

1) is false or obscene; or

2) would lead to (or create the possibility of leading to) a deterioration in law and order; or

3) would prejudice the image of the State; or

4) would or may offend religious belief; or

5) incite hostility against any person or organisation,

this activity will be regarded as an offence, and the ICT Controller may make an order to block the communication flow.

5. OVERSIGHT OF THE USE OF POWERS

There are no oversight mechanisms mandated in law in relation to the above legislation. However, the government and the Bangladesh Telecom Regulatory Commission may exercise oversight.

The empowered law enforcement agency may bring a claim against any non-compliance with the rules mentioned above and there are stipulated penalties for first time, second time and third time failures.

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

Restrictions on network operators and service providers

There is no direct statutory restriction on publishing aggregated data on government requests for surveillance and censorship powers described above. However the Bangladesh Telecom Regulatory Commission may declare such data to be confidential, exercising its discretion under section 85(1) of the BTRA.

In addition, as the powers are exercised on the grounds of national security and public order, any information relating to the use of such powers is considered confidential information as it may be part of an investigation or used in judicial proceedings. An equivalent position is adopted under the Right to Information Act 2009, under which any information that is given in confidence to any law enforcement agency is excluded from publication under the scope of the Act.

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

7.1 Information & Communication Technology Act, 2006 (the "ICT Act")

As referred to above, under section 46 ICT Act, where the ICT Controller is satisfied that it is necessary in the interest of:

(a) the sovereignty or integrity or security of the state;

(b) friendly relations with foreign states;

(c) public order;

(d) preventing incitement to the commission of any offence punishable under the ICT Act; or

(e) the investigation of any offence

it may, by order, direct any law enforcement agency of the government to intercept, any information transmitted, through any computer resource. This is an exception to the general rule of maintenance of privacy and secrecy of information in Bangladesh that may permit the interception of information in any computer resource. Where the information is such that it ought to be divulged in the public interest, the Controller may require disclosure of such information to law enforcement agencies. This may include information falling into the above categories.

In such circumstances the law enforcement agency appointed by the Controller, can direct a subscriber or any person in charge of a computer resource to extend their facilities to decrypt the information (s.46(2)). This section also provides for interception, monitoring and decryption for the investigation of cybercrimes. The Controller may, by notification in the Official Gazette or Electronic Gazette, declare any computer, computer system or computer network to be a protected system and authorize select law enforcement agencies officials to secure access to the protected systems (s.47).

All matters falling under Section 46 and 47 are dealt with by the Controller by serving notice and the Controller can impose penalties under s. 52 and 53 of the ICT Act.

Under sections 48 to 52, the relevant cybersecurity penalties are as follows:

(a) For failure to furnish document, return and report, a fine of up to 10,000 Taka;

(b) For failure to file a return, information, book etc., a fine of up to 10,000 Taka;

(c) For a failure to maintain books of accounts or record, a fine up to Taka two lakhs;

(d) For a breach of any given instructions, a fine up to 10,000 Taka; and

(e) For contravention of any provision of the ICT Act, a fine of up to 25,000 Taka.

(f) Under the ICT Act, there are eight main cybercrimes (summarised in 7.2 to 7.9 below).

7.2 Damage to a computer, computer system or computer network

Where an individual, without permission of the owner or any person who is in charge of the computer, computer system or computer network in question, carries out one of the following acts, he commits an offence under s. 54 of the ICT Act:

(a) accesses or secures access to a computer, computer system or computer network, for the purpose of destroying information or retrieving or collecting information or assisting another to do so;

(b) downloads, copies or extracts any data, computer database or information from a computer, computer system or computer network, including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or virus into a computer, computer system or computer network;

(d) willingly damages or causes to be damaged in a computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of a computer, computer system or computer network;

(f) denies or causes of the denial of access to any person authorized to access a computer, computer system or computer network by any means;

(g) provides assistance of any kind to facilitate access by another person to a computer, computer system or computer network, in contravention of the provisions of the ICT Act or rules or regulations made thereunder;

(h) for the purpose of advertisement of goods and services, generates or causes the generation of spam or sends unwanted electronic mails without the permission of the originator or subscriber; or

(i) charges the services availed by one person to the account of another by tampering with or manipulating any computer, computer system or computer network.

Should an individual commit any of the crimes described above, their actions are punishable by a fine of up to Taka 1 million (USD12,500) and/or a prison term of 7-14 years.

7.3 Tampering with computer source code

Where a person intentionally or knowingly conceals, destroys or alters (or intentionally or knowingly causes another person to conceal, destroy or alter) any computer source code used for a computer, program, system or network, when the source code in question is required to be kept or maintained by a law in force at that time, they will have committed a cybercrime under s.55.

A breach of Section 55 is punishable by a fine of up to Taka 0.3 million and/or imprisonment for a term of up to three years.

7.4 Hacking with a computer system

Under Section 56, a person is guilty of an offence of hacking if they;

(a) with the intent to cause, or knowing that they are likely to cause, wrongful loss or damage to the public or any person, destroy, delete or alter any information residing in a computer resource or diminish its value or utility or affect it injuriously by any means; or

(b) cause damage through the illegal access to any computer, computer network or any other electronic system which does not belong to them.

Hacking offences are punishable by a fine of up Taka 10 million (USD125,000) and/or a prison term of 7-14 years.

7.5 Punishment for publishing false, obscene or defamatory information in electronic form

According to Section 57, it is an offence to deliberately publish or transmit (or cause to be published or transmitted) on a website or in an electronic form, any material which is false and obscene or where its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all of the relevant circumstances, to read, see or hear the matter contained or embodied within the material. Section 57 also considers hacking to include deliberately publishing or transmitting (or causing to be published or transmitted) any material on a website or in an electronic form, which may undermine law and order, prejudice the image of the state or a person, offend religious belief or incite hostility against any person or organization.

This offence is punishable by a fine of up to Taka 10 million (USD125,000) and/or a prison term of 7-14 years.

7.6 Punishment for unauthorized access to protected systems

Under s.61 it is an offence to secure or attempt to secure access to a 'protected system' as designated by the ICT Controller.

Such an offence is punishable by a fine of up to 1 million Taka (USD12,500) and/or a prison term of 7-14 years.

7.7 Punishment for misrepresentation and obscuring information

Under Section 62, a person making any misrepresentation to, or suppressing any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, commits a criminal offence.

The punishment for misrepresentation and obscuring information is a fine of up to 0.2 million Taka (USD 2,500) and/or a prison term of up to two years.

7.8 Disclosure of confidentiality and privacy

According to Section 63, it is an offence where any person who, in pursuance of any of the powers conferred under the ICT Act or rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material and discloses such material to any other person without the consent of the person concerned.

Where an individual does disclose confidential and private information in breach of this section, he/she will be liable to a fine of up to 0.2 million Taka (USD 2,500) and/or a prison term of up to two years.

7.9 Punishment for publishing false or fraudulent digital signature certificates

Under s. 64 and 65 of the ICT Act, the offence of publishing false or fraudulent digital security certificates is punishable by a fine of up to 0.2 million Taka (USD 2,500) and/or a prison term of up to two years.

Cases relating to the above offences are heard by the Cyber Tribunal of Bangladesh and decisions thereof may be appealed at the Cyber Appellate Tribunal. Under the general judicial regime decisions may also be challenged in the Supreme Court of Bangladesh (ss. 68, 69, 82 and 83 of the ICT Act).

7.10 S.4 of the ICT Act states that if any person commits an offence under the ICT Act from outside Bangladesh using a computer, computer system or computer network located in Bangladesh, the ICT Act will apply as if the entire process of the offence took place in Bangladesh. Furthermore, if any person from within Bangladesh commits an offence under the ICT Act outside of Bangladesh then the Act applies as if the entire process of the offence took place in Bangladesh.

7.10 Upcoming Digital Security Act

The Government is working with a draft Digital Security Act to bring more control over dealings with offences related to cybersecurity. The draft has approval from the Cabinet of Ministers, however, is expected to be further amended and to be placed in the parliament for enactment in late 2017. The Act mandates for the creation of a new Government agency under the act in the name of Digital Security Agency with necessary workforce with a view to fulfilling the purposes of the Digital Security Act.

As per the act there would be a Director General of the Digital Security Agency and the government will appoint additional director general, director, deputy director and assistant direct as well as other officers. If the Director General is pleased that it is expedient and necessary to give directions for the interests of protecting the sovereignty, integrity, security of Bangladesh and friendly relationship of Bangladesh with other countries, public discipline and security, he/she can give directions to law enforcement agencies of the government by order mentioning written reason for obstructing the broadcast of information through any computer resource. The Director General will have the power to:

- take the possession of any computer, computer programme, computer system or computer network or any digital device, digital system or digital network or any programme, information, data which have been stored in any computer or compact disc or removable drive or any other way or access into the same;
- require any person or organization supply the transfer of information or data;
- do whatever is reasonably required for fulfilling the purposes of the act.

In addition, the proposed act declares the following as offences:

- Offences against the Critical Information Infrastructure (punishment: 14 years' imprisonment and / or 10m Taka fine).
- Forgery regarding computer or digital devices (punishment: 5 years' imprisonment and/or 0.3m Taka fine).
- Fraud regarding computers (punishment: 5 years' imprisonment and/or 0.3m Taka fine).
- Non-compliance with the direction of the director general in an emergency (punishment: 5 years' imprisonment and/or 0.3m Taka fine).
- Digital or cyber terrorist activities (punishment: up to life imprisonment and/or 10m Taka fine).
- Violating confidentiality (punishment: 5 years' imprisonment and/or 1m Taka fine).
- Pornography (punishment: 7 years' imprisonment and/or 0.5m Taka fine).
- Defamation, publication of false and obscene material, causing religious offence (punishment: 5 years' imprisonment and/or 0.5m Taka fine).
- Inciting hostility and deterioration of law and order (punishment: 7 years' imprisonment and/or 0.7m Taka fine).

Law stated as at 31 January 2017.

BULGARIA – 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 Bulgarian law.

1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

1.1 Law on Electronic Communications 2007 (the "LEC")

Article 304 states that undertakings which provide public electronic communications networks and/or services must ensure that they are set up in a way which allows for interception of electronic communications in real time and real time access to data related to a specific call. Where this data cannot be provided in real time, the data should be provided to the State Agency for Technical Operations and to the State Agency for National Security as soon as possible after the termination of the call. The interception procedure should be carried out in accordance with the Law on Special Intelligence Means.

Subject to Article 305, the undertakings which provide public electronic communications networks and/or services provide, commission and maintain, at their own expense, one or several interception interfaces by which intercepted electronic communications can be transmitted to the facilities of the State Agency for Technical Operations and of the State Agency for National Security. In addition they must ensure that they are set up in a way which allows for transmission of intercepted electronic services to these facilities over fixed or switched lines. The technical parameters, configuration and conditions for maintenance of the interception interfaces should be coordinated with the State Agency for Technical Operations and approved by its Chairman.

Interception must be conducted in a way which excludes the possibility of illegal interference in, and ensures protection of, the information related to the interception. Intercepted electronic communications are received only by the State Agency for Technical Operations and by the State Agency for National Security in compliance with the Law on Special Intelligence Means (Art. 309).

1.2 General Requirements for Provision of Public Electronic Communications (the "Requirements") (issued in 2008)

The Requirements were issued by the Commission for Communications Regulation on the grounds of Article 73 LEC. In accordance with Article 19 of the Requirements, the undertakings that provide public electronic communications networks and/or services are obliged to cooperate for the safeguarding of public interests, defending national security and ensuring electronic communications for defence needs and in national emergencies (crises).

In pursuance of this obligation and depending on the network used or services provided by a particular undertaking, it is obliged to set conditions, at its own expense, for interception of electronic communications by providing interfaces for the needs of the national security and public order. For the purposes of complying with these obligations, undertakings cooperate with competent state authorities, such as the State Agency for National Security, and implement the relevant interfaces that transmit electronic communications to these agencies.

1.3 Law on Special Intelligence Means 1997 (the "LSIM")

The LSIM sets out the terms and conditions, procedures for use and application and the control related to the use of special intelligence means (which includes interception and other ancillary covert activities) and the results obtained via these means. Under the LSIM, special intelligence means are used to prevent or detect intentional grave crimes, as listed in Article 3 (such as spying, sabotage, terrorism, murder, computer crimes, theft, etc.), where the relevant circumstances cannot be established in any other way or would be disproportionately difficult to establish by any other means.

The following government authorities have the right to request

the use of special intelligence means and to use the data collected and the material pieces of evidence retained: the National Police Directorate General, Organized Crime Fighting Directorate General, Border Police Directorate General, Internal Security Directorate General, the specialized directorates (with the exception of Technical Operations Directorate) and the territorial directorates of the State Agency for National Security, and the regional directorates of the Ministry of Interior, Military Information and Military Police services with the Minister of Defence and the National Intelligence Service. For some specified crimes, requests can also be made by prosecutors from the relevant Regional Prosecutor's Offices. In case of use of special intelligence means for preventing of terrorism, the request can be made by the Chief Prosecutor of the State, the Chairman of State Agency National Security, the Chairman of National Intelligence Service, the Director of Military Information Service or deputies authorised by them as well as by the Chief Secretary of the Ministry of Interior (Article 13).

Interception under the LSIM can only be undertaken where there is a grounded written request from the heads of the respective authorities, the aforementioned officials or by a supervising prosecutor. The requests should contain certain statutory requisites (such as facts substantiating the view that a grave crime has been committed, the proposed time period for the use of interception, and activities undertaken so far within the investigation). The request should be submitted to the Chairman of the Sofia City Court, of the respective district or military court or of the specialized criminal court or to a deputy empowered by that Chairman who will authorize or refuse the use of special intelligence means (Article 14 and Article 15). In addition and unless there are exceptional circumstances, once the use of special intelligence means has been authorised by the relevant court, the chairman of the State Agency for Technical Operations issues a written order for enforcing the relevant special intelligence means.

Interception may only be conducted by the relevant departments of the State Agency for Technical Operations or the Technical Operations Directorate of the State Agency for National Security, in accordance with the LSIM. However, in a limited number of cases, interception may be conducted by the National Intelligence Service and by the intelligence services of the Ministry of Defence – in the sphere of their competence and by the Ministry of Interior – where an undercover officer of the Ministry participates in a relevant investigation of crimes where the use of special intelligence means is permitted (Article 20).

1.4 Penal Procedure Code 2006 (the "Code")

Pursuant to Article 172(3) of the Bulgarian Penal Procedure Code, computer information service providers (a term which encompasses communication service providers) are under an obligation to provide assistance to the court and pre-trial authorities in the collection and recording of computerized data through the use of special intelligence means (including interception). The use of special intelligence means is limited to the purposes of investigating intentional grave crimes (those for which the law provides punishment by imprisonment for more than five years, life imprisonment, or life imprisonment without substitution, such as spying, sabotage and murder), where the relevant circumstances cannot be established in any other way or would be disproportionately difficult to establish by any other means. Interceptions under the Code are conducted pursuant to the LSIM.

Under the Code, where interception is required in a pre-trial investigation, a grounded written request for the use of special intelligence means is made by the supervising prosecutor to the court. The administrative head of the relevant Prosecutor Office making the request is also notified. The request should contain the following information listed in Article 173:

(i) information about the crime, the investigation of which requires use of special intelligence means;

(ii) a description of the activities conducted within the investigation so far and the results thereof (so that the judge can assess if interception is the only remaining method available to collect data and evidence);

(iii) information relating to the individuals that will be the subject of the interception;

(iv) information on the operational investigative methods (that the request is for interception);

(v) the time period for use of interception (this is as a rule two months, but can be extended to six months); and

(vi) the reasons why this method must be employed, and why the information required cannot be acquired in any other way, or that there would be extreme difficulties related to acquiring it in another way.

Authorization of the request is given by a ruling of the Chairman (or explicitly authorized deputy Chairman) of the respective court. On the grounds of the authorization, the Head of the State Agency for Technical Operations (or an authorized deputy head), or the Head of the State Agency for National Security (or an authorized deputy head) or the Chief Secretary of the Ministry of Interior, may issue a written order for the interception to take place in compliance with LSIM.

1.5 Law on the Ministry of Interior 2014 (the "LMI")

The LMI provides that, in executing its powers related to defence of citizens' rights and freedom, prevention and investigation of crimes, defence of national security, safeguarding the public order, etc. the investigative bodies of the Ministry of Interior are authorized to use different methods. If it refers to special intelligence means, such activities should be performed under the rules of LSIM.

1.6 Law on the State Agency for National Security 2008 (the "LSANS")

The LSANS sets out the statutory basis that, in carrying out their various investigative activities, the structures of the State

Agency for National Security are authorized to use special intelligence means (including interception) in accordance with the LSIM (Article 123). Furthermore, they are authorized to require other state authorities, legal entities (such as companies) and individuals to provide the information necessary to carry out their obligations and such entities and persons are required to immediately provide any information that has been obtained or acquired in relation to a request made in pursuance of the powers of the State Agency for National Security (Article129). There is no definition of "immediately".

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1Law on Electronic Communications 2007 (the "LEC")

Undertakings providing electronic communications networks and/or services have statutory obligations to keep safe the confidentiality of communications. However, due to the prevailing public interest, the LEC provides for three specific types of disclosure of communications data: (a) interception under the procedures of LSIM as this includes the provision of communications data related to the intercepted communication; (b) provision of information under Article 310 of the LEC (which would be requested prior to carrying out the interception); (c) disclosure of particular retained data. The specific cases under (b) and (c) are not related to disclosure of the content of communication.

The relevant details with respect to the interception obligation have been mentioned in Section 1.1 above.

Pursuant to Article 310 of the LEC, before implementation of lawful interception takes place, the State Agency for Technical Operations and the State Agency for National Security require the undertakings that provide public electronic communications networks and/or services to provide:

1) data to establish the identity of the subscriber, the number or another identifying feature of the electronic communications service;

2) information about the service and the characteristics of the electronic communications system used by the subject of interception and provided by the undertakings that provide public electronic communications networks and/or services; and

3) information about the technical parameters of the transmission

to the facilities of the State Agency for Technical Operations.

In addition, the undertakings that provide public electronic communications networks and/or services must retain for a period of six months (which may be extended by a period of up to three months by permission of the court), certain data generated or processed in the course of their activities which can be used to trace and identify: the source of a communication; its destination, date, time and duration; the type of the communication; the communications terminal equipment of the user or what purports to be a communications terminal equipment of the user, and the Cell ID (Article 251b). Pursuant to Article 251b, paragraph 3, other data, including data disclosing the content of the communications, may not be retained in accordance with this data retention procedure.

Access to these data is limited to the needs of national security, the prevention, detection and investigation of grave crimes. Cell ID data can be used also for search and rescue of individuals under the Disaster Protection Act (upon receiving information that a person is, or may be, in risk threatening his/her life or health) (Article 251b, paragraph 2).

The retained data may be accessed by the authorities listed in Art. 251c (such as certain directorates of the State Agency for National Security, the Ministry of Interior and the Ministry of Defence, as well as the National Intelligence Service) when such data is necessary for the performance of their duties.

Subject to LEC, the retained data is accessed after a grounded court order is given by the Chairman of the respective regional court (or a judge authorised by him). In the event of immediate danger from specific categories of crimes (terrorism, forgery with the intention to facilitate terrorism, etc.) the undertakings providing electronic communications have to provide access immediately and directly – based on the request of the head of the competent authority. The request is then notified to the competent court and if the court denies access to the retained data, the electronic communications provider shall be notified and the component authority has to destroy the data obtained so far.

Alternatively, for the purposes of criminal investigations and proceedings under the Penal Procedure Code, the data are provided to the pre-trial investigation authorities and the court in compliance with such Code.

2.2 Penal Procedure Code 2006 (the "Code")

Article 159a sets out the procedures for accessing the data retained under the LEC for criminal investigations and proceedings under the Code. Under the Code, access to the retained data (being the same as under LEC) is granted by the undertakings providing electronic communications networks and/or services either upon request of the court (when the relevant proceedings are in their court stage), or on the grounded order of a judge from the competent first instance court, issued under a substantiated request of the prosecutor supervising the pre-trial procedure (during the pre-trial stage). Such data may be accessed for the purpose of investigating intentional grave crimes.

3. NATIONAL SECURITY AND EMERGENCY POWERS

3.1 Law on Electronic Communications 2007 (the "LEC")

In accordance with Article 301 of the LEC, the undertakings that provide public electronic communications networks and/or services must ensure the capability for the provision

of electronic communications in case of natural disasters as defined by the Disasters Protection Act, and in case of a declaration of a state of martial law, state of war or state of emergency in the meaning of the Law on Defence and Armed Forces of the Republic of Bulgaria.

In order to safeguard national security, undertakings which provide electronic communications networks and/or services must ensure the competent authorities have access to the network and/or the services provided, as well as the ability to use electronic communications over the network free of charge in case of an imminent threat to national security. In addition, if there is an imminent threat to national security or in a limited number of specified scenarios (detecting, identifying and defusing explosive devices and explosive substances; freeing hostages; detecting and preventing the use of national radio spectrum against the state etc.), the competent authorities may block the use of electronic communications services by using technical means. The competent authorities in this case are the State Agency for National Security, certain bodies of the Ministry of Interior, the Military Police Service and National Security Office.

In accordance with Article 302 and Article 120, if a state of martial law or a state of war is declared or in case of danger to national security, the Commission for Regulation of Communications (following a decision/request of a competent authority) can temporarily suspend the validity of permits for radio spectrum frequencies. When such decisions are made the regulator is authorised to forbid the use electronic equipment or radio frequency spectrum for civil needs as long as this is needed.

Under Article 303, the undertakings which provide electronic communications networks and/or services and have assigned wartime tasks must use and maintain their electronic communications network in a state of readiness to provide of electronic communications in the event of natural disasters as defined by the Disasters Protection Act, or of a declaration of a state of martial law, war or emergency as defined by the Law on Defence and Armed Forces of the Republic of Bulgaria.

3.2 Disaster Protection Act 2006

In accordance with Article 30, the undertakings which provide electronic communications have the obligation to assist the Ministry of Interior and the National Emergency Call System 112 to carry out communications during natural disasters. In addition, pursuant to the latest amendments of Art 38:

(a) upon the request of the operating centres of the integrated rescue system, the electronic communications providers must transmit free of charge, immediately and without altering the content and the meaning any urgent information, required to protect the population, in accordance with the established agreements;

(b) in case of receipt of information for an individual who is in, or may be in a position that poses risks to his/her life or health, the undertakings which provide public electronic communications networks and/or services have to provide Cell ID data retained in compliance in LEC within 2 hours after the request of the Chief Directorate "Fire Safety and Population Protection" within the Ministry of Interior.

3.3 Law on Defence and Armed Forces in the Republic of Bulgaria 2009

When a state of war, state of martial law or a state of emergency has been declared, the state authorities and the armed forces may take control over the facilities of the critical statutory infrastructure. The critical statutory infrastructure and activities are defined and identified by Decree No 181 of the Council of Ministers, dated 20th of July 2009 for determining of the strategic objects and activities critical for national security, including amongst other things, mobile and fixed communications services. Three of the undertakings which provide such services (Mobiltel, Bulgarian Telecommunications Company and Telenor Bulgaria) are identified as part of the critical statutory infrastructure, meaning that the relevant state authorities and the armed forces may take control over their facilities (Article 123).

3.4 Law on the Ministry of Interior 2014 (the "LMI")

The police authorities may issue orders to state authorities, organizations, legal entities and natural persons where this is necessary for performance of their functions. As a general principle the orders are in writing, where possible and as long as they would be understandable by the persons to whom the order is directed. The orders have minimum content determined by the law and are subject to appeal (Article 64). Furthermore, in the process of detection, identification and deactivation of explosive devices and explosive substances, police authorities may block electronic communications by using technical means (Article 90).

3.5 Counter Terrorism Law 2016

In the framework of an anti-terrorist operation and on the request of the competent authority, the undertakings providing electronic communication services must temporarily restrict the use of electronic communications services by a particular user (Article 39).

Where under particular circumstances (terrorist act resulting in multiple deaths and injuries, substantial property damage or damage to the economy of the country, etc.) the National Assembly or the President have declared a state of emergency, the undertakings providing electronic communications networks and/or services must (i) ensure the provision of electronic communications, (ii) provide the competent authorities with access to the network and/or the services as well as free of charge use of electronic communications through the network and (iii) temporarily suspend the operation of the electronic communications networks if ordered so by the competent authorities. Further terms and conditions as well as the relevant procedures for ensuring electronic communications upon declaration of a state of emergency are yet to be set forth by the Council of Ministers on a proposal by the Minister of Transport, Information Technology and

Communications in consultation with the relevant competent authorities.

4. CENSORSHIP

The right of expression, regardless of the media used, is a fundamental right set out in the Bulgarian Constitution, and censorship is illegal (Article 39 and Article 40 of the Constitution of the Republic of Bulgaria). There are, however, a number of statutes which provide for the blocking of certain information in particular circumstances, as set out below.

4.1 Law on Electronic Communications 2007 (the "LEC")

In specific scenarios, the competent bodies within the Ministry of Interior, the State Agency for National Security, the Military Police Service and the National Security Office may block, by technical means, the use of electronic communications services (Article 301, paragraph 3). These scenarios include, but are not limited to, the following: counter terrorism activities; detecting, identifying and defusing explosive devices and explosive substances; freeing hostages; detecting and preventing the use of national radio spectrum against the state and when national security is threatened.

In addition, upon declaration of a state of martial law or a state of war and following the decision of a competent authority, the Communications Regulation Commission may suspend the validity of issued permits for radio spectrum frequencies and prohibit the use of radio equipment and radio spectrum for civil needs (Article 302 and Article 120).

The undertakings providing public electronic communications services may furthermore collect, process and use electronic communications data retained for detecting and terminating unauthorized use of electronic communications networks and facilities, where there is reason to consider that such actions are being performed and this has been claimed in writing by the affected party or by a competent authority (Article 256, Paragraph 1).

4.2 Law on Electronic Commerce 2006

On the grounds of Article 15(b) and Article 16, paragraph 2 (related to providers of caching or hosting services), the providers of information society services must either delete the information stored in the course of provision of the services or block access to such information pursuant to an order of a competent authority. The law does not specify the meaning of "competent authority", however this would likely be interpreted to encompass all authorities with the power to lawfully require or implement blocking of access to content or those engaged in investigation and prevention of crimes, such as, the police at the Ministry of Interior, or the State Agency for National Security.

4.3 Law on the Ministry of Interior 2014 (the "LMI")

Under Article 64, paragraph 2, police authorities are entitled to issue mandatory orders (as a general rule written, where possible and as long as they are understandable by the persons to whom the order is directed) if necessary to fulfil their functions. The orders must contain certain information determined by the law and are subject to appeal. Furthermore, in the process of detection, identification and deactivation of explosive devices and explosive substances, police authorities may block electronic communications by using technical means (Article 90).

4.4 Law on Gambling 2012

Web access may be blocked under a resolution of the State Commission on Gambling (the "Commission") if a violation of the gambling rules is not remedied within three days of a resolution setting out the violating websites. For the purposes of blocking the access, a request is then made by the State Commission on Gambling to the Chairman of the Sofia Regional Court and a writ of the court is published on the website of the Commission. The blocking of the websitewebsite is performed by the relevant undertakings within 24 hours of the publication of the Court order at the website of the Commission.

4.5 Counter Terrorism Law 2016

If websites with content that incite terrorism or which spread information about the perpetration of terrorism are detected, both the Ministry of Interior and the National Security State Agency may request the blocking of access to such websites. The request should be justified and is subject to judicial control by the Chairman of the Specialized Criminal Court, who on his/her turn may deny the blocking or issue an ordinance for blocking. The court orders for blocking the access are published immediately on the official websites of the Ministry of Interior and the National State Security Agency. As of the publication all undertakings providing electronic communications networks and/or services must immediately block access to the websites listed in the court ordinance. The blocking should last until the court resolution has been repealed and information for authorizing the access to the websites has been published on the official websites of the Ministry of Interior and the National State Security Agency (Article 32).

5. OVERSIGHT OF THE USE OF POWERS

5.1 Law on Special Intelligence Means 1997 (the "LSIM")

Control over the legitimate use of interception carried out under the LSIM is undertaken by the Chairman of the State Agency on Technical Operations if the special intelligence means are used by that agency; by the Chairman of the State Agency for National Security, if the special intelligence means are used by the units of the agency; or by the Minister of Interior where special intelligence means are used in relation to the investigation involving undercover officer of the Ministry of Interior (Article 34a).

National Bureau Oversight

The monitoring of the procedures for authorization, enforcement and use of special intelligence means, the storage and destruction of information obtained through special intelligence means, as well as of protection of citizens' rights and freedoms against illegal use of special intelligence means is carried out by the National Special Intelligence Means

Control Bureau (the "National Bureau") (an independent government agency, consisting of five people elected by the Parliament for five years and supported by an administrative office).

The National Bureau has the authority to request information from the state authorities that carry out functions related to special intelligence means (including interception), to issue mandatory instructions related to improvement of the regime of use and enforcement of special intelligence means, as well as of the storage and destruction of the information obtained through such means, and to citizens against which special intelligence means have been applied illegally. Where special intelligence means and storage and destruction of the data procured through use of these means have been used illegally, the National Bureau will notify the prosecutor's office and the heads of the controlling bodies and departments mentioned in the paragraph above.

Committee Oversight

Article 34h of the LSIM provides for a Committee for Oversight of the Security Services, the Deployment of Special Surveillance Techniques and the Access of Data under the Law on Electronic Communications. This is a standing Committee constituted at the Bulgarian National Assembly under the Rules of Organization and Procedure of the National Assembly.

The Committee carries out parliamentary oversight and monitoring with respect to the procedures of authorization, enforcement and use of special intelligence means and the storage and disposal of data obtained.

5.2 Law on Electronic Communications 2007 (the "LEC")

Regulatory Oversight

Under Article 261a of the LEC, the Personal Data Protection Commission (the "Commission") is the supervisory authority in relation to security of the data retained under Art. 251b, Paragraph 1.

The Commission has the right within its supervisory competence to require information from the undertakings which provide public electronic communications networks and/or services and issue binding instructions that are subject to immediate execution. In addition, each year the Commission provides the Bulgarian Parliament and the European Commission with summarized statistical information on:

1) the cases in which retained data has been provided to the competent authorities;

2) the time elapsed between the initial date on which the data has been retained and the date on which the competent authorities requested the provision of the retained data; and

3) the cases where requests for retained data could not be executed.

Committee Oversight

The National Assembly, acting through a committee designated by the Rules of Organization and Procedure thereof (Committee for Oversight of the Security Services, the Deployment of Special Surveillance Techniques and the Access of Data under the Law on Electronic Communications), carries out parliamentary oversight and monitoring of the procedures for permission and implementation of access to the traffic data retained under the LEC, as well as for protection of citizens' rights and freedoms against lawful access to any such data. In pursuance of its activities, the committee has the right to:

1) require information from the authorities competent to request access to retained traffic data from the providers of electronic communications, as well as from the Personal Data Protection Commission;

2) inspect the procedure and the manner of storage of the retained traffic data, the requests and the orders as well as the procedure for destruction of the traffic data;

3) access the premises of the requesting authorities and the undertakings providing electronic communications networks and/or services; and

4) prepare annual reports on the audits held and to propose improvement of the procedures for retention and processing of the retained traffic data.

The Ministry of Interior, the Ministry of Defence, State Agency National Security, State Agency Intelligence Service and the Chief Prosecutor must prepare by not later than March 31 of the year following the reporting year an annual report summarising the requests made, the court orders issued, the data obtained and the retained data destroyed. The report is provided to the parliamentary committee. If, based on such reports, the committee has established any non-compliance, the latter notifies the prosecutor's office, the respective non-compliant authority and the undertakings providing electronic communications networks and/or services. The latter have the obligation to implement corrective measures and inform the committee in due term of such measures and their implementation. The committee notifies the affected data subjects ex officio, unless this could prevent reaching of the purposes of processing (national security related, prevention, detecting, investigation of crimes, etc.).

5.3 Law on the Ministry of Interior 2014 (the "LMI")

The orders of the Minister of Interior for temporary restriction of certain activities may be appealed by the individuals or legal entities affected within seven days via the Minister of Interior before the Supreme Administrative Court (the "Court"). In this case the procedures under Administrative Procedure Code are followed.

In addition to the court procedures, the Administrative Procedure Code allows for individuals or organisations to contest administrative instruments before the superior

administrative body (for example, the administrative procedure for contesting orders by the police, in relation to safeguarding human rights and civil liberties would be before the Director of Police, of officer that has issued the order). Appeal before the superior administrative body is not a prerequisite for further court appeal before the respective court.

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

6.1 Law on the Protection of Classified Information 2002 (the "LPCI")

Information relating to the lawful use of special intelligence means (including interception) is deemed to be a state secret as set out in Appendix 1 of the LPCI. Access to classified information and state secrets is granted on a need-to-know basis to persons that have permission, and this permission may be granted by the State Commission for the Security of Information (Article 8) or the State Agency for National Security (Article 11). Therefore, publication of such information may not be published unless authorised by these agencies.

6.2 Constitution of Bulgaria

Under Article 5, paragraph 5 of the Bulgarian Constitution, all laws must be published. Therefore, there is no power for the government to prevent anyone from publishing the laws to which they are subject.

7. CYBERSECURITY

7.1 Cybersecurity Legislation

As of the date of this report, the only instrument directly relating to cybersecurity in Bulgaria is the National Strategy for Cybersecurity "Cyberproofed Bulgaria 2020" (the "CB") which was approved on 18 July 2016. However the CB only contains guidance with respect to the national strategy for cyber-security and does not detail the provisions applicable to electronic communications providers.

Pursuant to the National Strategy on Cyber-security, it is the following authorities that are obliged to implement the national strategy:

1) The National Coordinator on Cyber-security, who heads the elaboration and implementation of the National Strategy on Cyber-security, the national plan for cyber-security activities and carries out other tasks related to cyber-security; and

2) The National Cyber-security Situation Centre, organized by the National Situation Centre, that carries out permanent monitoring of the cyber-security national framework and coordinates the reaction and response to any cyber-security crisis. Specific operative and technical activities are carried out by the respective CERT/CSIRT (who are in place permanently) and the emergency response teams (who are usually organised in a more ad hoc fashion).

In contrast to the first group of authorities that have powers to apply national legislation in the event of a crisis or emergency situation, the second group of organizations mainly hold functions related to the monitoring, early identification, prevention and coordination of crisis control.

No executive powers have been explicitly laid down by Bulgaria's cyber-security legislation. To the extent that cyber-security is an element of national security, the national security and emergency powers provided to the respective authorities apply. For more details, please refer to the National Security and Emergency Powers and Censorship sections of this report.

The rights and obligations of electronic communications providers with respect to the information security and integrity of their networks are therefore regulated more specifically by the Law on Electronic Communications (the "LEC"). Pursuant to the LEC, electronic communications providers are additionally obligated to take appropriate technical and organizational measures to manage any security risk their networks or services are faced with. Such measures should ensure a level of security appropriate to the risk in question by taking into account the nature of the problem and the cost of implementing the protective measures.

Where there is a breach of cyber-security or the security integrity of a network or service has been impaired to a degree that has had a significant impact on its operation, the electronic communications providers have to notify the Communications Regulation Commission ("CRC") immediately of this breach (Article 243 et seq.). The CRC has the authority to:

- inform the public of any cyber-breach or require the provider to do so in cases that the Regulator determines disclosure of the breach is in the public interest;
- inform the Minister of Transport, Information Technology and Communications of any cases of a cyber-security breach;
- request the providers of electronic communications networks or services to provide the information necessary for the CRC to assess the security and/or integrity of the services and networks thereof, including any internal documented security policies;
- audit the security of an electronic communications network or service through a qualified independent body; and
- issue binding instructions to the electronic communications providers to take specific measures to ensure the security of the networks and the services they provide.

In the event of a risk of a cyber-security breach related to an electronic communications network or service, the electronic communications provider must inform their subscribers of this risk in an appropriate manner. In doing so, providers must provide their subscribers with the relevant information of the said risk, the necessary remedies that will be applied and the costs involved.

Also note that under the LEC, there is no specific sanction to be applied where there has been a breach of a provider's security obligations. However the general pecuniary sanction for non-compliance with the general requirements for the provision of the services shall apply - a fine ranging between BGN 3,000 (approximately EUR 1,500) and BGN 15,000 (approximately EUR 7,500).

Whilst Bulgarian legislation does not contain codified statutory rules regulating cyber-security, to the extent the cyber-security is an element that makes up part of Bulgaria's national security, the principle statutory regulation (which is applicable to national security), the Law on the Management and Functioning of the National Security Defence System, shall apply. Particular aspects of cybersecurity are also regulated by other statutes, including:

(i) the Disaster Protection Act which outlines the rights and obligations of the authorities and citizens in the occurrence of disasters caused by nature and/or human conduct;

(ii) the Law on Electronic Government which contains provisions relating to the information security of the state administration's infrastructure;

(iii) the Law on Protection of Classified Information which regulates the information security of networks storing and transmitting classified information;

(iv) the Counter Terrorism Law which contains the rights and obligations of authorities and citizens in the event of terrorist attacks; and

(v) the respective subsidiary legislation and international instruments that have been ratified and been entered into force by the Republic of Bulgaria.

8. CYBERCRIME

The Bulgarian Penal Code sets forth several types of computer crimes

Statutory Reference	Offence	Penalty
Article 319a	Copying, using or obtaining access to computer data in a computer system without permission, where such permission is required	Fine up to BGN 3,000 (approx.: EUR 1,500)
	In the case of two or more individuals acting in prior agreement to commit the above crime	Imprisonment of up to 1 year and a fine up to BGN 3,000 (approx.: EUR 1,500)
	Where the crime is repeated or in regard to data for creating of electronic signature	Imprisonment of up to 3 years and a fine of up to BGN 5,000 (approx.: EUR 2,500)
	Where the crime concerns state secrets or otherwise protected information	Imprisonment of 1 to 3 years, unless a stricter punishment is not provided for
	Where severe consequences flow from the commission of the crime	Imprisonment from 1 to 8 years
Article 319b; Article 319c	Installing, modifying, deleting or destroying a computer program or computer data, without the consent of the person administering or using the computer system, provided that the case is not considered insignificant	Imprisonment of up to one year or a fine from up to BGN 2,000 (approx.: EUR 1,000)
	Where the commission of the crime has resulted in significant damage or severe consequences	Imprisonment of up to two years and a fine up to BGN 3,000 (approx.: EUR 1,500)
	Where the intent behind the commission of the crime was material benefit	Imprisonment from one to three years and a fine up to BGN 5,000 (approx.: EUR 2,500)
	Where the crime is in regard to data that are provided in compliance with the law, electronically or on electronic, optical or another carrier	Imprisonment of up to two years and a fine from up to BGN 3,000 (approx.: EUR 1,500)
	Where the intent behind the commission of the crime was to prevent the fulfilment of an obligation	Imprisonment of up to three years and a fine from up to BGN 5,000 (approx.: EUR 2,500)
Article 319d	Introducing a computer virus in a computer system or in a computer network	A fine of up to BGN 3,000 (approx.: EUR 1,500)
	Where the crime results in significant damage or is repeated	Imprisonment of up to three years and a fine from up to BGN 1,000 (approx.: EUR 500)
Article 319d, para 2	Introducing a computer program, other than a virus, which is intended to disrupt the work of a computer system or a computer network or to discover, erase, delete, modify or copy computer data without permission, where such permission is required	Fine of up to BGN 3,000 (approx.: EUR 1,500)
	Where the crime results in significant damage or is repeated	Imprisonment of up to three years and a fine from up to BGN 1,000 (approx.: EUR 500)

Statutory Reference	Offence	Penalty
Article 319e	Disclosing passwords or codes for access to a computer system or to computer data which results in personal data or information which qualifies as a state secret or otherwise protected information being revealed	Imprisonment of up to one year
	In cases where the crime is committed for material purpose or severe consequences have resulted thereof	Imprisonment of up to three years
Article 319f	Breach of particular provisions of the Law on Electronic Document and Electronic Signature upon provision of information services In cases where the crime is committed for material purpose	Fine from up to BGN 5,000 (approx.: EUR 2,500), unless a harder fine is not provided for

The penalties outlined above are imposed by the competent Bulgarian court.

The Bulgarian Penal Code applies to foreigners in the following specific cases:

1) where the cyber-crime has been committed in the territory of the Republic of Bulgaria;

2) where a foreigner has committed the cyber-crime abroad, yet the interests of the Republic of Bulgaria or of Bulgarian citizens have been affected; or

3) where the applicability of the Penal Code has been provided for in an international agreement, to which the Republic of Bulgaria is a party.

The rulings of a court imposing penalties for any breach of the Penal Code are subject to the same appeals procedure as applicable in the general criminal procedure, i.e. a three instance court procedure with the rulings of the first instance court being subject to appeal before the competent appellate court and the rulings of this court being subject to appeal to the Supreme Court of Cassation.

Law stated as at 20 February 2017

DENMARK – 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 Danish law.

1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

1.1 Consolidation Act on Electronic Communications Networks and Services, 2014

(Bekendtgørelse af lov om elektroniske kommunikationsnet og –tjenester (Act no. 128 of 7 February 2014, (the "Tele Act"))

The Tele Act, in conjunction with the Retention Order (described in section 2 of this report below), sets out a telecom provider's obligation to make data available to the police, both by providing access to retained data and by providing interception capabilities.

According to section 10 Tele Act, a network operator or service provider must ensure that all technical equipment and systems used to provide an electronic communication network or service to end-users are set up in such a way that the police may intercept current communications and conduct mobile phone surveillance. In this context, mobile phone surveillance means the procurement of data that makes it possible to locate a mobile phone on a continuous basis as long as it is turned on.

Under section 10, the systems of the network operator or service provider must be set up to allow interception and immediate transmission of telecommunications data to another EU member state under the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01).

In the case of a data interception request, the network operator or service provider must provide the IP-address, MAC-address or any similar identifier of the device making or receiving the communications that are to be intercepted.

1.2 Administration of Justice Act 2016 (Bekendtgørelse af lov om rettens pleje (Act no. 1257 of 13 October 2016, (the "AJA"))

Section 783 sets out the general rule that the police must obtain a court order and present it to the relevant network operator or service provider before an interception may be made. The application for a court order must comply with the following conditions:

- there must be specific indications that communications, using the method of communication that is to be intercepted, are taking place to or from a suspect of the investigation;
- the interception must be decisive to the investigation; and
- the alleged offence must have a sentence of at least six years' imprisonment, or be one of a list of specified offences, such as desertion from the military or possession of child pornography.

In addition, interception must always be proportionate to the purpose for which it is to be used.

Section 783(4) provides for an exception to the general rule. Where obtaining a court order would cause a delay that would defeat the purpose of carrying out the interception, the police may conduct the interception without obtaining a court order first.

However when this happens, the police must, as soon as possible and no later than 24 hours from the interception, submit an application for a court order for the interception as set out above. The court then determines whether the interception was lawful, and if so, the length of time it should be allowed to continue. If the court finds that the interception was not lawful, it is obliged to notify the Ministry of Justice, which has statutory authority to investigate any breach of this

process by the police.

1.3 Centre for Cybersecurity Act 2014 (Lov om Center for Cybersikkerhed (Act no. 713 of 25 June 2014, (the "Centre for Cybersecurity Act"))

The Danish Centre for Cybersecurity (the "Centre") is the national IT Security authority who has established a "network security service" (the "Service") to which companies whose businesses have a socially important function, such as pharmaceutical companies, food companies and companies that administer administrative IT-systems, as well as most public institutions, can apply for connection. Through the Service, the Centre aims to discover, analyse and prevent cybersecurity breaches within the connected entities in order to maintain a high level of information security in Denmark, for example, to prevent hacking.

In order to connect to the Service, the relevant company or public institution must enter into an affiliation agreement with the Centre. Once connected, the Centre may process content and traffic data in the networks of the connected entities to the Centre's Service, without obtaining a court order, so long as such interception is made with the purpose of ensuring a high level of information security. The Centre cannot connect a company or institution to the Service unless such a company or institution actively asks to be connected. Further cybersecurity related provisions under the Centre for Cybersecurity Act are explained in section 7 of this report.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Executive Order on the retention and storage of traffic data by providers of electronic communications networks and services (Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) (No. 988 of 28 September 2006, as ame nded by executive order of amendment no. 660 of 19 June 2014, (the **"Retention Order"**))

The Retention Order governs what data must be stored by a network operator or service provider.

Under section 5(1), a network operator or service provider must retain the following data about a user's access to the internet:

(a) the allocated user identity (for example, the user name or customer number);

(b) (b) the telephone number which has been allocated to the user's communications as a part of a public electronic communication network;

(c) (c) the name and address of the subscriber or registered user to whom an IP address or user identity or telephone number had been allocated at the time of communication; and

(d) (d) the time of the beginning and the end of a communication.

Under section 5(2), a network operator or service provider providing wireless access to the internet must retain data concerning the local network's precise geographical or physical location and the identity of the user's communication equipment. Data retained under the Retention Order must be stored for one year.

2.2 Consolidation Act on Electronic Communications Networks and Services 2014 (the "Tele Act")

According to section 10 Tele Act, a network operator or service provider must ensure that all technical equipment and systems used to provide an electronic communication network or service to end-users are set up in such a way that the police may obtain access to information about telecommunications traffic in the form of;

- telecommunications data, meaning information regarding which telephones or similar communications devices have been connected to a specific telephone or similar communications device either prior to or after the issue of an authorising court order; and
- extended telecommunications data, meaning information listing the connections made by the telephones or similar communication devices within a defined area (described by the police) either prior to or after the issue of an authorising court order (this would typically be information from cell phone masts).

Under section 13, when required by the police, network operators and service providers are obliged to disclose to the police data which identifies an end-user's access to electronic communications networks or services. This includes static information such as a designated IP-address, address, or phone number that the network operator or service provider has assigned to the end-user. The police can lawfully obtain this information without obtaining a court order.

A network operator or service provider which offers encrypted data as an integrated part of its service is obliged to decrypt an encrypted communication when complying with a court order. If, however, encryption has taken place outside of the services offered by the network operator or service provider, it will be the police's own responsibility to remove any encryption from the provided data.

It is prohibited for network operators and service providers to retain content data. However, the police may retain, access and review the content of a person's correspondence, subject to the rules on lawful interception outlined in section 1 of this report above.

2.3 Administration of Justice Act 2016 (the "AJA")

The police may obtain access to historic telecommunications data in accordance with chapter 71 AJA. Section 783 sets out the general rule that, in order to do so, the police must obtain a court order and present it to the relevant network operator or service provider. The application for a court order must comply with the following conditions:

- there must be specific indications that communications are

taking place to or from a suspect of the investigation using the method of communication that is to be intercepted;

- access to the relevant telecommunications data must be decisive to the investigation; and
- the alleged offence must have a sentence of at least six years' imprisonment, or be one of a list of specified offences, such as desertion from the military or possession of child pornography.

In addition, access to historic telecommunications data must be proportionate to the purpose for which it is to be obtained.

3. NATIONAL SECURITY AND EMERGENCY POWERS

3.1 Radio Frequencies Act

(Act no. 1100 of 10 August 2016, Lov om radiofrekvenser (the "RFA")), and the Order on maritime radio services in extraordinary situations (Bekendtgørelse om de maritime radiotjenester i ekstraordinære situationer (Executive order no. 916 of 13 November 2002, (the "Maritime Radioservice Order"))

According to section 32 RFA and the Maritime Radioservice Order, the Danish Navy Operative Command may, in situations of crisis, war, catastrophes and other extraordinary situations, shut down the coastal radio station and thus shut down normal public correspondence over coastal radio.

In accordance with section 33 RFA, the Danish Energy Agency (the "DEA"), who acts as the regulatory supervisory authority for the telecoms industry under the remit of the Danish Ministry of Energy, Utilities and Climate, may prohibit the use of certain radio frequencies when the safety of the state demands it.

Under section 6(5) of the RFA, the police, when exercising a power to disturb or interrupt radio and telecommunications that is granted under section 791(c) of the Administration of Justice Act, may do so without first obtaining a licence or other authorisation from the DEA to use the radio frequency spectrum in question.

3.2 Network and Information Security Act

(Net- og informationssikkerhedsloven (Act no. 1567 of 25 December 2015, (the "Network and Information Security Act"))

In 2016, the Network and Information Security Act, a framework regulation, was enacted. Following this the Centre has drafted new regulations on network and information security, including the 'Information and Security Order' (Bekendtgørelse om Informationssikkerhed og beredskab i net og tjenester) (Executive Order Number 567 of 1 June 2016) under which a provider of public electronic communications networks or services is responsible for information security in its network based on a documented risk management process. A provider must identify any possible cybersecurity risks and using this risk assessment, implement proper measures to ensure the accessibility, integrity and confidentiality of its networks and services. Further cybersecurity obligations under the Network and Information Security Act are set out in section 7 of this report.

The Information and Security Order also governs a provider's obligations in relation to crisis management in emergency situations, such as large disasters, where it may be necessary to implement remedial actions in regards to networks and services in order to maintain critical services. Also, 'significant commercial providers' shall ensure that the Centre can make contact with them in connection with an emergency situation at any time. Centre may also direct such providers to participate in national or international crisis management practices.

In addition to the Information and Security Order, the Centre has also issued the "Emergency Operator Order" (Bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.) (Executive Order Number 564 of 1 June 2016), which sets out certain actions that providers must take in emergency situations, including the prioritization of calls in mobile networks, the provision of secure access to a telephone network and the prioritization of re-establishment of certain parts of a provider's network as directed by the Centre.

4. CENSORSHIP

4.1 The Constitutional Act of the Kingdom of Denmark, 1953 (the "Constitution")

Under section 77 of the Constitution, censorship and other measures prohibiting freedom of expression are prohibited.

4.2 Gaming Act 2016 (Act no. 1494 of 6 December 2016, Bekendtgørelse af Lov om spil, (the "Gaming Act"))

As a general rule, government agencies do not have the authority to block IP addresses. The Telecommunications Industry Association (Teleindustrien) (a private industry organisation of which the majority of Danish network operators and service providers are a part) has stated that network operators and service providers need only carry out DNS blocking following an authorising court order and that they will not carry out any DNS blocking based solely on requests from intellectual property rights holders, government agencies or other third parties.

The only current exception to this is the Danish Gaming Board who may request that a network operator or service provider blocks a website containing illegal gambling systems.

5. OVERSIGHT OF THE USE OF POWERS

5.1 Judicial Oversight

Insofar as a court order is required to intercept or access retained data or to block any website, the competent court will have oversight of this procedure.

5.2 Executive Order on the retention and storage of traffic data by providers of electronic communications networks and services (the "Retention Order")

The Retention Order was issued by the Danish Ministry of Justice (the "Ministry"). The Ministry oversees the compliance of network operators and service providers with the retention and storage requirements specified in the Retention Order. Non-compliance with the Retention Order may lead to financial penalties imposed by the Ministry.

5.3 Consolidation Act on Electronic Communications Networks and Services 2014 (the "Tele Act")

Following the Danish general election in 2015, it was decided to relocate much of the regulation of the telecoms sector from the Ministry of Business and Growth to the Ministry of Energy, Utilities and Climate and accordingly move the main parts of the regulatory authority from the Danish Business Authority (the "DBA") (an agency under the Ministry of Business and Growth) to the Danish Energy Agency (the "DEA") (an agency under the Ministry of Energy, Utilities and Climate).

Consequently, the DEA is now the main regulatory authority responsible for electronic communications who administers the legal framework within this area. This includes promoting information technology security, promoting individual and public use of information technology and the Internet, developing the telecoms market, administering scarce resources, protecting consumers, and protecting public information and communications business.

However, certain areas still remain under the Danish Business Authority (the "DBA"), including matters within telecoms regulations relating to personal data and sector-specific competition regulation.

Both the DEA and DBA therefore oversee compliance by network operators and service providers with the Tele Act. For example, the DEA ensures that electronic communication networks are set up to enable interception by the police. Under chapter 33, section 79 Tele Act, both the DEA and the Telecommunications Complaints Board (the "Board") may enforce compliance and issue financial penalties for breaches of the Tele Act described in this report.

The Board comes under the remit of the Ministry of Energy, Utilities and Climate. Decisions taken by the DEA may be brought before the Board and any decisions taken by the Board may be appealed to the High Court.

5.4 Administration of Justice Act 2016 (the "AJA"))

For the Danish police to conduct a lawful interception, section 783 AJA contains the general rule that they must first obtain a court order to do so. This rule is subject to certain exemptions which allow for an interception to take place without an order provided that the police make a submission to the court within 24 hours of the interception for its retrospective examination. If the court rules that the interception was not in compliance with law, it then notifies the Danish Ministry of Justice of the matter. The Ministry of Justice has statutory authority to investigate such non-compliance by the Danish police.

5.5 Centre for Cybersecurity Act 2014 (the "Centre for Cybersecurity Act")

For interceptions made in accordance with the Centre for Cybersecurity Act, it is the Centre for Cybersecurity (the "Centre") who is solely responsible for determining whether or not to intercept. The Centre is placed under the Danish Defence Intelligence Service, which sits within the Danish Ministry of Defence. In relation to the data processed by the Centre, the Danish Data Protection Act 2000 will not apply (nor does it apply generally to the police). However, the Minister of Justice and the Minister of Defence appoints a supervisory board that supervises the Centre's use and processing of personal data.

5.6 Radio Frequencies Act 2016 (the "RFA") and the Maritime Radioservice Order 2002

Under the RFA, the DEA determines whether consideration to the safety of the state demands the prohibition of the use of certain radio frequencies.

Under the Maritime Radioservice Order, the Danish Navy Operative Command determines whether the coastal radio station should be shut down.

5.7 Gaming Act 2016 (the "Gaming Act")

The Danish Gaming Board oversees compliance by network operators and service providers with the Gaming Act.

5.8 Network and Information Security Act

(Net- og informationssikkerhedsloven (Act no. 1567 of 25 December 2015, (the "Network and Information Security Act"))

The Centre oversees compliance by network operators and service providers with the Network and Information Security Act. The Centre is placed under the Danish Defence Intelligence Security and Intelligence Service which sits within the Danish Ministry of Defence.

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

Restrictions on network operators and service providers

There are no restrictions on whether a network operator or service provider may publish aggregate data regarding government powers of interception, disclosure of communications data or censorship as described in this report. Equally, there are no restrictions on whether a network operator or service provider may publish descriptions or analysis regarding such powers.

Aggregate data published by government agencies

Government agencies do not publish aggregate data in relation to the use of their powers of interception, disclosure of communications data or censorship as described in this report.

7. CYBERSECURITY

7.1 Consolidation Act on Electronic Communications Networks and Services,

(Act Number 128 of 7 February 2014 (the "Tele Act")) and The Executive Order on Personal Data as regards Public Electronic Communications Services, (Executive Order Number 462 of 23 May 2016 (the "EOPD"))

Pursuant to section 7(1) Tele Act, owners of electronic communications networks and providers of electronic communications networks or services and their employees and former employees shall not be entitled, without authorisation, to disclose or utilise information about an individual's use of the network or service in question, or the content thereof that comes to their knowledge in connection with the provision of these electronic communications networks or services. The owners and providers of such networks and services shall furthermore "...take the measures necessary to ensure that information about [an]other persons' use of the network or service or the content thereof will not be available to unauthorised persons."

Section 8 Tele Act contains a framework provision on personal data which has resulted in the EOPD. Pursuant to the EOPD, providers of public electronic communications networks or services must continuously ensure that they implement proper technical and organizational measures to control potential security breaches relating to the personal data that they process. Such measures shall, as a minimum, ensure:

1) (i) that authorized personnel are allowed access to personal data for legitimate purposes only;

2) the protection of stored personal data and personal data in transmission against accidental or unlawful destruction, loss or alteration and against unauthorized or illegal storing, processing, access, or distribution; and

3) that a security policy for personal data is prepared.

4) Providers of public electronic communications networks or services are further obligated to inform their end-users of any event that poses as a particular risk to their personal data security.

All providers must inform the Danish Business Authority (the "DBA") of an actual breach of personal data security within 24 hours of its occurrence. In doing so, they must state in detail the character of the breach, its consequences, and any counter measures they have initiated. Furthermore, if the breach of personal data security can be expected to violate the personal information or privacy of an end-user, the provider must also immediately inform the end-user of this breach.

7.2 The Danish Act on Network and Information Security

(Act Number 1567 of 15 December 2015 Lov om Net-og Informationssikkerhed (the "Network and Information Security Act"))

The Centre for Cybersecurity (the "Centre") has issued four Executive Orders under the Network and Information Security Act, including:

1) the Executive Order on Information Security and Emergency in Networks and Services (Bekendtgørelse om Informationssikkerhed og Beredskab i Net og Tjenester) (Executive Order Number 567 of 1 June 2016) (the "Information and Security Order")); and

2) the Executive Order on Information and Disclosure obligations regarding Network and Information Security" (Bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og Informationssikkerhed,Executive (Order Number 566 of 1 June 2016) (the "NIS Disclosure Order")).

Precautionary measures in terms of Information Security

In addition to the cybersecurity obligations referred to in section 3.2 of this report, under the Information and Security Order, providers of public electronic communications networks or services are responsible for their personal information security based on a documented risk management process.

Stricter rules apply for specific providers, including 'commercial providers' and 'significant commercial providers'. These providers are required to additionally prepare an information security policy approved by their management, based on an international standard such as the DS/ISO/IEC 27001. They are also required to establish an information security organization which is responsible for managing all of the provider's relevant security tasks. Significant commercial providers are additionally subject to a number of general information security obligations, including the obligation to ensure awareness of current information security threats and to implement security plans for the protection of specific critical net components and systems.

Pursuant to section 25-26 of the Information and Security Order, the Centre may issue specific directions to 'commercial providers' and 'significant commercial providers' provided that these directions are of 'material public interest'. Such directions may require the provider to ensure:

1) the security clearance of specific personnel;

2) the retention of certain employees necessary to perform the risk management processes; and

3) the performance of an independent safety valuation.

A disclosure regime is set out in the NIS Disclosure Order. Pursuant to section 7, providers of public electronic communications networks and services are required to notify the Centre of any security breaches that result in significant implications for the operation of their networks and services. A significant implication for the operation of networks and services will occur if the stated threshold values, in terms of the duration of the breach as set out in section 8, are reached (for example, for internet access, the threshold would be met if the security breach results in 10,000 user hours being affected and where the effect lasts longer than one hour). The Centre may in this context issue a specific direction to a provider that it shall inform the general public of the security breach in question provided that the publication is considered as being of public interest, as per section 11.

7.3 Centre for Cybersecurity Act 2014

(Lov om Center for Cybersikkerhed (Act no. 713 of 25 June 2014, (the "Centre for Cybersecurity Act"))

The main regulatory supervisory authorities for the telecoms industry in Denmark in terms of cybersecurity are the Centre for Cybersecurity (the "Centre") and the Danish Business Authority ("DBA"). As referred to in section 1.3 of this report, the Centre for Cybersecurity Act regulates the Centre's 'network security service' (the "Service"), which analyses internet traffic to and from the authorities and companies that are connected to this Service in order to detect any signs of intrusion.

In the event of an unauthorised intrusion and potential cyber-attack, the Centre conducts an advanced analysis to expeditiously determine the nature and severity of the threat. In the case of a specific cyber-attack, the Centre will directly inform the targeted organization and advise them of the measures to take to respond to the attack.

In addition to the above, the Centre also informs and advises on the preventive measures that may be taken and issues guidelines and recommendations on the strengthening of cybersecurity efforts and the prevention of cyber-attacks to Danish public authorities and private companies.

The executive powers provided for under the cybersecurity legislation governing the Centre do somewhat affect an individual's general rights, in particular their right to privacy. However, balancing such human rights with the protection of cybersecurity and resistibility against cyber threats in Denmark has been the subject of well-considered public debate and ultimately such legislation has been deemed necessary and proportionate. Nonetheless, the relevant authorities are subject to clear guidelines in their operations. For example, the Centre may only process data in connection with the 'Network Security Service' provided it is in compliance with the specific guidelines as of 30 June 2014.

Moreover, the 'Danish Intelligence Oversight Board' is a special independent monitoring body that oversees the Centre and ensures that it processes information about natural persons in connection with the Service in a manner that is compliant with the relevant legislation, including when intervening in secret communications. Any decisions made by the Centre may be appealed to the Danish Ministry of Defence.

Non-compliance with the legislation on network and information security is subject to a fine imposed by the Centre or the DBA.

8. CYBERCRIME

The Danish Criminal Code (Straffeloven) (Consolidation Act Number 1052 of 4 July 2016, (the "CC")) considers the following activities as cyber offences under Danish law:

Statutory Reference	Offence	Penalty
Criminal Offences against Property		
Section 291	Attack on IT-system Described as destroying, damaging or removing any property belonging to another person. Note that attacks on IT-systems may comprise of knowingly sending computer viruses and 'denial-of-service-attacks' (i.e. where the owner or holder is cut off any access to operate their IT-system)	A fine or imprisonment for a term not exceeding one year and six months
Section 293(2)	DDoS ('Distributed Denial of Service') Described as wrongfully preventing another person from disposing of an item in full or in part / exposing a computer system to a DDoS (i.e. Distributed Denial of Service) attack If the offence is committed in a systematic or organised manner or in otherwise particularly aggravating circumstances	A fine or imprisonment for a term not exceeding one year Imprisonment for up to two years
Section 279a	Data Fraud Described as wrongfully editing, adding or deleting data or programs for electronic data processing or otherwise wrongfully attempting to influence the output of such data processing, in order to obtain an unlawful gain for himself or others For example where a perpetrator, who gets into an IT-system for account transfers unlawfully transfers amounts to his own account and withdraws the cash	Imprisonment for approximately one year and six months
Various acts harmful to the General Public		
Section 193	Comprehensive interference in the operation of Information Systems Described as wrongfully causing comprehensive interference with the operation of any public transport means, public postal service, telegraph or telephone service, radio or television broadcasting system, information system or service providing public utility of water, gas, electricity or heating Note that this criminal offence is generally targeted at addressing attacks on large IT-systems of social importance (e.g. attacks on high street banks or other big companies) but also attacks on central internet-functions such as DIX and hostmaster It is of no importance how the specific attacks are accomplished. Both hacking minor controlled attacks in the form of virus and physical attacks by way of interruption of a teleconnection will fall within the scope of this criminal offence If the offence is committed through gross negligence	A fine or imprisonment for a term not exceeding six years A fine or imprisonment for a term not exceeding six months

Statutory Reference	Offence	Penalty
Criminal Offences concerning means of payment and evidence		
Section 169, 171 and 301	Described as criminal offences relating to the means of payment and evidence If the act was of a particularly aggravating nature	A fine or imprisonment for a term not exceeding two years Imprisonment for up to six years
Invasion of Privacy		
Section 263(1)	Monitoring or wire-tapping of telecommunication Described as, wrongly, by means of a listening device, secretly wiretapping or recording statements made in solitude, telephone conversations or other conversations between other persons	A fine or imprisonment for a term not exceeding six months
Section 263(2)	Hacking Described as wrongly gaining access to any data or programs of another person intended for use in an information system If the offence is committed with the intent to obtain or become acquainted with the business secrets of an enterprise, or if other particularly aggravating circumstances apply (e.g. organized criminal activities) If the offence is committed in a systematic or organised manner	 A fine or imprisonment for a term not exceeding one year and six months Imprisonment for a term not exceeding six years Imprisonment for a term not exceeding six years

The Danish Ministry of Justice (Justitsministeriet) is responsible for creating legislation concerning the criminal law and is the part of the Ministry who issues any amendments to the Criminal Code.

As a general rule, acts falling within Danish criminal jurisdiction are acts committed within the Danish state, which implies that any criminal offence committed in Denmark can be prosecuted in Denmark, regardless of the perpetrator's nationality.

However, pursuant to section 9 CC, if the criminality of an act depends on or is influenced by an actual or intended consequence, the act is also deemed to have been committed at the place where the effect occurred or where the offender intended the effect to occur (referred to as the 'Principle of Impact'). Consequently, a cybercrime committed outside of Denmark may still end up being subject to Danish criminal jurisdiction.

Any victim (person or a company) affected by the commission of a cybercrime may report this to the Danish Police, and more specifically the National Police Cyber Crime Centre ("NC3"), a special section of the Danish Police. It will be the Danish Prosecution Service (Anklagemyndigheden) however that will make the decision as to whether to press charges against the perpetrator. On a practical note, whilst the prosecutors will work closely with the police officers that investigate the criminal offence, it is the prosecutors who will have to assess whether a case is likely to stand up in court. If so, the prosecutor is to appear before a District Court judge and attempt to have the perpetrator convicted. Any decision made by the District Court judge may be appealed to the High Court or the Supreme Court (which is the highest tier of the Danish legal system).

Law stated as at 21 February 2017.

HUNGARY – 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 Hungarian law.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

1.1 National Security Service Act

Act 125 of 1995 on the National Security Services (the "National Security Service Act"); Act 34 of 1994 on the police (the "Police Act") and Act 19 of 1998 on Criminal Proceedings (the "Criminal Proceedings Act") give the competent court, and in the case of the intelligence agencies under the National Security Service Act, the Minister of Justice, the power to authorise the interception of a person's communications following an application made by the relevant intelligence agency or law enforcement agency ("LEA").

1.2 Electronic Communications Act

Under s.92(1) of Act 100 of 2003 on Electronic Communications (the "Electronic Communications Act"), electronic communications service providers in Hungary are required to cooperate with organisations authorised to conduct covert investigations and to use their facilities in their electronic communications systems so as not to prevent or block covert investigations, e.g. interceptions.

In addition under s.92(2) of the Electronic Communications Act, at the written request of the National Security Services, electronic communications service providers are required to conclude an agreement with the National Security Services. Under s.17(2) of the Government decree No. 180/2004 on the rules of cooperation between electronic communication service providers and authorities authorised for secret data collection (the "Government Decree on Cooperation") any such agreement should be concluded within 60 days after receipt of the written request of the National Security Services. The agreement should address the application of the means and methods of covert investigation operations.

1.3 Criminal Proceeding Act

Under s.202(6) of the Criminal Proceedings Act, interception by LEAs may only be conducted if it reasonably appears that obtaining evidence by other means would be unlikely to succeed or would involve unreasonable difficulties, and there is probable cause to believe that evidence can be obtained by the interception.

Under s.71 of the Police Act and s.203 of the Criminal Proceedings Act, the competent court can issue an order for interception. Under s.57-58 of National Security Services Act, the competent court or the Minister of Justice, can issue an order for interception.

1.4 Government Decree on Cooperation

The Electronic Communications Act and the Government Decree on Cooperation requires electronic communications service providers to cooperate with LEAs and intelligence agencies in relation to covert investigations and set up and maintain interception equipment.

Under s.3(a) of the Government Decree on Cooperation, electronic communications service providers must ensure, among other things, that all conditions necessary for the implementation of tools in relation to covert investigation operations are satisfied; for example, through the provision of a lockup room where the necessary equipment can be placed, non-stop technical assistance, if required, etc.

Under s.3(3) and s.6(3) of the Government Decree on Cooperation, LEAs and intelligence agencies can install technical devices so that they have direct access to the networks of electronic communications service providers, without the personal assistance of the employees of the service providers.

2. DISCLOSURE OF STORED COMMUNICATIONS DATA

2.1 Electronic Communication Act

Under s.157(10) of the Electronic Communications Act, intelligence agencies, courts, public prosecutors and investigation authorities including the police and (in relation to certain criminal offenses) the National Tax and Customs Authority, have the power to acquire the metadata relating to customer communications including traffic data, IMEI number, service use information and subscriber information, but not the content of the communications. Under s.157(8)-(9) and (11) of the Electronic Communications Act a further range of authorities, including the Hungarian Competition Authority, the Hungarian National Bank (the "MNB") acting as financial supervisory authority, and the Consumer Protection Authority are entitled to request metadata but only if such authorities are conducting investigations in relation to suspicious activities listed in these sections.

Under s.3/B and 13/B(1) of Act 108 of 2001 on electronic commerce and information society services ("E-Commerce Act"), if an application service provider offers encrypted services (other than end-to-end encryption), it is required to disclose the content of the communication or conversation to the authority carrying out any covert investigation, if so requested, and must store the metadata of the communication or conversation for 1 year and must disclose it to the authority carrying out any covert investigation, if so requested.

"Application service provider" is defined as a natural person or legal entity who or which provides access to software or hardware through an electronic communication network, provides a software application or any related services through a specific software or web portal to multiple users, limited or unlimited in time, for monthly or use-based consideration or for free.

Under s.157(8) of the Electronic Communications Act, in the case of certain financial regulatory proceedings conducted by the MNB acting as financial supervisory authority, electronic communications service providers may be requested to disclose to the MNB certain data such as the subscriber's name, address, telephone number or other identifier of the subscriber terminal, call logs or details of other services provided.

Under s.157(8a) of the Electronic Communications Act, in the case of certain anti-trust proceedings or other proceedings relating to unfair business-to-consumer commercial practice, conducted by the Hungarian Competition Authority (the "HCA"), electronic communications service providers may be requested to disclose to the HCA certain data such as the subscriber's name, address, telephone number or other identifier of the subscriber terminal, call logs or details of other services provided.

Furthermore, if the agreement or concerted practice aims, directly or indirectly, at price fixing, sharing the market or fixing quotas, the HCA may also require the disclosure of further data such as the IMEI number of the mobile telephone used, identification data regarding the network and cell providing the service in the case of mobile telephone services; or in the case of IP networks, the identifiers used.

Under s.71 of the Police Act and s.203 of the Criminal Proceedings Act, the competent court can make an order for interception, while under s.57-58 of National Security Services Act, the competent court or the minister of justice can issue an order for the interception (including to granting access to the content of stored customer communications (e.g. voicemail)).

Under s.68 of the Police Act, if a request is made by the police in relation to serious crimes (as is defined under s.68), the supply of data cannot be refused.

Under s.11(5) of the National Securities Services Act, the competent minister investigates complaints made in relation to the activities of the intelligence agencies.

In addition, lawful process and transfer of personal data is also monitored by the National Authority for Data Protection and Freedom of Information, the president of whom hears and investigates complaints about any alleged misuse of personal data.

3. NATIONAL SECURITY AND EMERGENCY POWERS

Except as already outlined in this report, government agencies do not have any other legal authority to invoke special powers in relation to access to a communication service provider's customer data and/or network on the grounds of national security.

3.1 Electronic Communications Act

Under s.37(1) of the Electronic Communications Act, for the protection of human lives, health, physical integrity, or for the protection of the environment, public safety and public policy, or for the prevention of dangers exposing significant threats to a broad range of users, or that directly jeopardize the operations of other service providers and users, the National Media and Info-communications Authority (the "NMHH") may pass a resolution on the prohibition of the provision of any service or the use of radio frequencies.

4. OVERVIEW OF USE OF THE POWERS

No appeal can be submitted against the relevant resolution of the NMHH in relation to the prohibition of the provision of any service or the use of radio frequencies, however, judicial review of the resolution can be requested from the competent court.

Interception is subject to the prior, or in urgent cases the subsequent, approval of the court/minister. No appeal can be submitted against an order of the court/minister unless the interception resolution is in relation to an ongoing investigation under the Criminal Proceedings Act.

5. CYBERSECURITY

5.1 Government Decree No 187 of 2015 ("Decree 187")

Decree 187 governs the duties and powers of the authorities supervising all electronic information systems and covers the role of the information security supervisor.

According to s.25(1), it is the National Directorate General for Disaster Management (the "Directorate General") who supervises the security of electronic information systems belonging to critical national infrastructures.

Under s.7 of Act 50 of 2013 on the Electronic Information Security of Government and Municipal Bodies ("EISA") (see below), operators of critical national infrastructures should classify their electronic information systems according to each system's security level, with reference to its confidentiality, integrity and availability. In addition, under s.9 EISA, operators should also classify themselves according to their security readiness in relation to the relevant electronic information system. These system and operator classifications must be reviewed at least once every three years.

S.19 of Decree 187 states that the Directorate General has the power to verify such classifications and operators' compliance with the related legal requirements. These are set out in s7-13 of the EISA and establish the criteria for security levels of systems and classification of operators as well as obligations in relation to security of information systems. The Directorate General may order the remedy of any deficiencies identified, monitor the effectiveness of such remedies and conduct a risk analysis, if necessary.

Moreover, under s.5(1) of Decree 187, the Directorate General is entitled to carry out inspections of operators' premises, alone or together with another authority. Accordingly, the Directorate General may:

(a) enter any premises relating to the information technology activity of an operator;

(b) carry out inspections on the data processing location or other premises relevant to information technology and review any documents, agreements, active or passive devices, information systems and security measures regarding electronic information security and make copies of any documents and agreements regarding electronic information security; and/or

(c) carry out technical investigations and have individual access to the information system for such investigations, if necessary.

Under s.20 of Decree 187, the Directorate General is entitled to take, order and monitor compliance of measures in order to protect the security of critical national infrastructure electronic information systems and the data contained therein from threats. Accordingly, the Directorate General is entitled to:

(a) supervise whether the operator of the electronic information system meets the legal safety requirements and complies with the related procedural rules;

(b) request the documents necessary to demonstrate compliance with the relevant requirements; and

(c) prepare an action plan for the elimination of the information system's vulnerability.

Moreover, according to s.6(3) Government Decree No 185 of 2015 ("Decree 185") which sets out the powers and duties of the Government Incident Management Centre and the rules for conducting the technical investigation of security incidents and vulnerabilities, it is the Directorate General who is designated to deal with threats and security incidents affecting the electronic information systems of critical national infrastructures.

The Director General's decisions are final. However, the affected ISPs may have recourse to courts through judicial review (in Hungarian: bírósági felülvizsgálat).

5.2 Act 100 of 2003 on Electronic Communications ("ECA")

Under s.92/B, providers of electronic communication services covered by the EISA, such as operators of critical national infrastructure, must report to the Special Service for National Security acting as the Government Incident Management Centre, all security incidents and threats affecting their electronic communication networks and services. Operators of electronic communication services must also notify their subscribers or users whose communication terminal equipment or information systems are affected by any such incident or threat, or which caused or threatened to cause the incident.

5.3 Act 50 of 2013 on the Electronic Information Security of Government and Municipal Bodies ("EISA")

Under s.16(2) of EISA, if an operator fails to meet the legal safety requirements and respect the related procedural rules, as set out in s.5-6 and in s.11-13 (safety requirements) and s.14-18 (procedural obligations), the competent authority shall request that the operator do so. Under s.2(6) of EISA and s.25(1) of Decree 187, the competent authority is the Directorate General. If the operator fails to comply with such a request, the authority may impose a fine, taking into consideration all of the circumstances of the case. Under s.13(3) Decree 187, the amount of this fine can vary between HUF 50,000 (approx. EUR 160) and HUF 5 million (approx. EUR 16,000). Such a fine may be imposed repeatedly if the operator continues to fail to comply with the authority's requests for compliance.

Furthermore, under s.13(2) Decree 187, the Directorate General is entitled to require operators to take immediate measures if the deficiency, failure or infringement of safety requirements threatens to cause a serious security incident.

6. CYBERCRIME

6.1 Act 100 of 2012 on the Criminal Code ("Criminal Code")

The Criminal Code sets out the following categories of criminal offences relating to cybercrime:

Statutory Reference	Offence	Penalty
375	Fraud through the use of an information system. Defined as where an individual, for the purpose of making an unlawful gain: (a) enters data into an information system; (b) alters or deletes data being processed therein; (c) renders such data inaccessible; or (d) interferes with the operation of the information system (e) and this results in damage.	Imprisonment for a maximum sentence of 3 years. The sentence is increased however if the fraudulent use of an information system: • caused significant damage or was committed by an organized criminal group or on a commercial basis causing greater damage, to an imprisonment term of 1 to 5 years; • caused particularly great damage or was committed by an organized criminal group or on a commercial basis causing significant damage, to an imprisonment term between 2 and 8 years; or • caused particularly significant damage and was committed by an organized criminal group or on a commercial basis causing particularly great damage, to a term of imprisonment of 5 to 10 years.
422	Unlawful acquisition of data. Defined as where an individual – for the purpose of unlawfully discovering personal data, private secret, economic secret or trade secret amongst other things: (a) unlawfully acquires and records (with appropriate technical device) data transmitted to another person through an electronic communication network, including an information system, or stored thereon, for the purpose of unlawfully obtaining personal data, private secrets, trade secrets or business secrets; (b) collects information other than the data indicated in point (a) above, in order to identify the investigator or the person cooperating in secret with the law enforcement agency or intelligence agency or the activity thereof; or (c) transmits or uses personal data, private secrets, trade secrets or business secrets acquired in the manners described at point (a) and (b) above.	Imprisonment for a maximum sentence of 3 years. If any of the above crimes were committed: • on a commercial basis; • under the guise of an official procedure; • by an organized criminal group; or • by causing a significant conflict of interest the sentence to imprisonment shall be for a term between 1 and 5 years.

Statutory Reference	Offence	Penalty
423	Breach of the information system and data breach. Defined as where an individual: (a) enters an information system without authorization by breaching or circumventing the technical measures ensuring the security of the information system, or stays in the system by going beyond the scope of their eligibility for access or infringes such eligibility; or (b) disrupts the functioning of an information system without authorization or by going beyond the scope of their eligibility for access or alters or deletes data in the information system or renders such data inaccessible by going beyond the scope of their eligibility for access.	Imprisonment for a maximum sentence of 2 years. Imprisonment for a maximum sentence of 3 years. If a crime under this section affects a significant number of information systems, the term of imprisonment shall be increased between 1 and 5 years. If it was committed against a public plant, the term of imprisonment shall be further increased to a term between 2 and 8 years.
424	Circumvention of technical measures ensuring information system security. Defined as where an individual: (a) creates, hands over, discloses or obtains a password or computer program or puts such a program on the market which is necessary to or facilitates the commission of a cybercrime indicated at s.375, 422(a) and 423 above; or (b) for the purposes of committing a cybercrime, makes their know-how relating to the creation of passwords and computer programs available to any third person, which is necessary to or facilitates the commission of a cybercrime indicated at s.375, 422(a) and 423 above.	Imprisonment for a maximum sentence of 2 years.

In Hungary the general law enforcement authority is the police therefore the above criminal proceedings are conducted by the police. The police refer the case to the public prosecutor who then decides about indictment at the criminal court (which is competent for the actual case). The competent court is usually a local district court.

If a criminal offence is committed 'for the good of a company' then there are measures which can be applied against the company itself. These include dissolution of the company, restricting its activity, or imposing a fine. However, these measures can only be applied if a private individual's criminal liability is established.

Act 104 of 2001 on the Criminal Measures Applied against Legal Persons provides measures which can be applied against a company if a private individual committed a crime and:

(a) the crime was committed with intent;

(b) the purpose of the crime was to gain financial advantage for the company, or resulted in such advantage, or the crime was committed with the assistance of the legal person; and

(c) either (i) the crime was committed by an executive officer, representative, employee or Supervisory Board member of the company within the scope of the latter's activity or (ii) the crime was committed by a member or employee within the scope of the latter's activity and the executive officer, the Supervisory Board member etc. could have prevented the crime if he had fulfilled his controlling or supervisory duties.

Measures against the company can also be applied if:

(a) the crime resulted in advantage for the legal person, or the crime was committed with the assistance of the legal person; and

(b) the executive officer, representative, employee, Supervisory Board member etc. of the company was aware of the commitment of the crime.

If a criminal court finds the executive officer of the company or another person mentioned above guilty and imposes punishment on them, the following measures can be applied against the company:

(a) dissolution of the company, provided that the intent behind establishing the company was to conceal committing a certain crime, or the actual activity of the company aims to conceal committing a certain crime; or

(b) restricting the activity of the company (e.g. the company may not participate in public procurement procedures, conclude concession contracts, receive a subsidy); and/or

(c) a fine, the maximum amount of which is three times the amount of the financial advantage gained or intended to gain, but at least HUF 500,000 (approx. EUR 1,600). If the amount of financial advantage cannot be determined then the court will estimate it.

Measures b) and c) above can be applied independently or conjunctively, whereas measure a) can only be applied independently.

7. CENSORSHIP OF COMMUNICATIONS

7.1. Web-blocking/filtering in general

In Hungary there are web-blocking/filtering obligations mandated by law under certain circumstances. These can be ordered based on (i) criminal law alone (temporary or permanent blocking), or (ii) administrative law (which is akin to gambling law)(temporary blocking). The obligation relates to ISPs and to search, cache and hosting providers.

The Hungarian Media and Communications Authority ("NMHH") offers a solution called the Technical Support System ("TSR"), which is intended for ISPs who do not want to develop their own web-blocking system. Furthermore, the NMHH operates a database (the "KEHTA Database") which contains blocking orders issued by courts or other authorities (the customs and tax authority, NAV). Service providers are obliged to connect to this database. All ISPs must register in the KEHTA database, but this is rather administrative for ISPs who joined TSR.

There are two legal bases for blocking orders:

(a) Criminal law: according to section 158/B(4) of the Criminal Proceedings Act, temporary blocking orders may require the temporary removal of electronic data or the blocking of access to such data. Removal can be ordered by the court in the case of criminal offences subject to public prosecution (in Hungarian 'közvádra üldözendő bűncselekmény'), provided that at the end of the criminal procedure permanent blocking can be ordered and such temporary blocking is necessary for preventing the continuation of the given offence.

On the other hand, according to s.158/D(1) of the Criminal Proceedings Act, blocking of access can only be ordered in case of child pornography, drug trafficking, encouraging substance abuse, misuse of a drug precursor, abuse of new psychoactive substances, offences against the state (spying, high treason etc.), terrorism and terrorism financing. Blocking can be ordered and an ISP must comply with such order, provided that the court had ordered the hosting provider to remove content without success.

(b) (Administrative (gambling) and then criminal law: according to s.36/G(1)-(2) of the Gambling Act (as defined below), in case of illegal gambling the NAV can order blocking of access to such content for 365 days. This is coordinated by NMHH by using of the KEHTA database. In principle, after 365 days, the blocking order expires.

However, under s.36/I(2)-(3) of the Gambling Act, the NAV terminates the blocking prior to such date of expiry if the reason for ordering the blocking does no longer exists or an order on permanent blocking as a permanent criminal sanction or temporary blocking as a criminal measure is being issued or implemented.

The NMHH notifies the service providers electronically of the content to be blocked. Providers must connect to the KEHTA Database unless they connect to internet exchange points via another provider which already connected to the KEHTA Database.

In addition, in case of illegal online gambling, the NAV publishes the content to be blocked on its website www.szf.hu under the tag "Hirdetmények" (in English: Announcements). The individual announcements are made available by NAV for a minimum of 15 days. Additionally, under s.36/J of the Gambling Act, a list of all blocked websites, service providers having committed illegal gambling activity and the number of the bank accounts used for organizing illegal gambling is also made available on www.szf.hu under the tag "Blokkolt honlapok" (in English: "Blocked websites").

7.2. Relevant laws for web-blocking/filtering

The relevant laws are included in different pieces of legislation:

(a) Criminal Code (Act 100 of 2012): s.77. – permanent blocking of electronic data as a permanent criminal sanction;

(b) Criminal Proceedings Act (Act 19 of 1998): s.158/B – temporary blocking of electronic data as a temporary measure, of which there are two kinds: (i) temporary removal of e-data (usually by a hosting provider) or (ii) temporary blocking of access to e-data (usually by an ISP, search or cache provider);

(c) E-Commerce Act (Act 108 of 2001): s.12/A – temporary or permanent blocking of access to e-data (by a hosting provider);

(d) E-Communications Act (Act 100 of 2003): s.92/A - temporary or permanent blocking of access to e-data (by an access provider / ISP); and s.159/B – tasks and powers of the NMHH in relation to temporary or permanent blocking including the operation of the KEHTA Database;

(e) NMHH Decree 19/2013 on connection of access providers / ISPs and search and cache providers to the KEHTA Database;

(f) Gambling Act (Act 34 of 1991): s.36/G – temporary blocking of e-data, providing of or access to which constitutes illegal gambling activity. This is valid for 365 days, however, the NAV may terminate the blocking prior to such date of expiry, if the reason for ordering the blocking no longer exists or an order on permanent blocking as a permanent criminal sanction or temporary blocking as a criminal measure is being issued or implemented; and

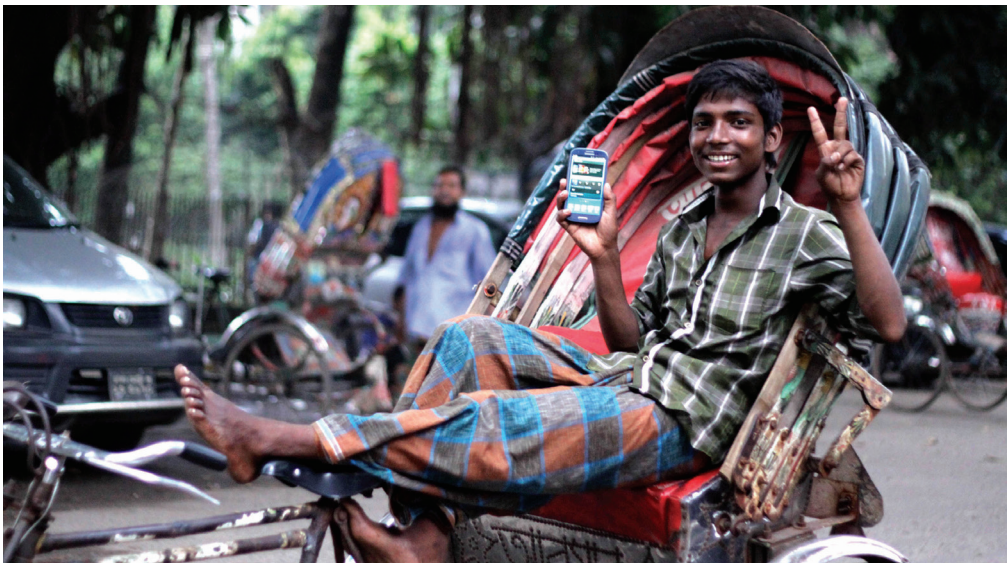
(g) BM Decree 23/2003 on detailed provisions of criminal investigations: s.87/A – temporary blocking of e-data, the task of investigative bodies (police, customs and tax authority, public prosecutor) in relation to temporary blocking of data.

Law stated as of 21 February 2017

INDIA – 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 and certain activities undertaken for reasons of national security or in times of emergency under the laws of the Republic of India.



1. LEGISLATIVE BACKGROUND

Indian Telegraph Act 1885 ("ITA Act")

This is the parent legislation governing telecommunications in India and the government grants the following licenses to service providers in accordance with the provisions of this Act:

Unified Access Service License ("UASL")

This is the license governing the provision of access services in India by entities granted licenses prior to 2013.

Internet Service Provider License ("ISP License")

This is the license governing the provision of internet services in India by entities granted licenses prior to 2013.

Unified License ("UL")

The Department of Telecommunications ("DoT") since 2013 issues the Unified License, which is an umbrella license covering all services such as access, internet, national long distance and international long distance. This implies that a service provider can provide all or any licensed telecommunications services under a single license by obtaining the relevant service authorisations under the Unified License. Current UASL and ISP licensees will have to migrate to the Unified Licence Regime on expiry of their existing licenses. For the purposes of this report, we have referred to all three major types of telecommunications licenses in existence today: the UL, the UASL and the ISP License, highlighting differences between them if relevant.

Information Technology Laws

The laws generally governing communications over the Internet are as follows:

Information Technology Act, 2000 ("IT Act")

This is the parent legislation governing information technology in India. It empowers the government to undertake various forms of electronic surveillance and censorship in accordance with procedures prescribed in the following rules:

IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ("Interception Rules")

These Rules specify the procedure the government must follow to intercept, monitor and decrypt electronic information stored, generated, transmitted or received in any computer resource.

IT (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 ("Traffic Data Rules")

These Rules specify the procedure the government must follow to monitor and collect traffic data or information for the purposes of cybersecurity.

IT (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ("Blocking Rules")

These Rules specify the procedure the government must follow to order the blocking of IP addresses.

IT Rules, 2011 ("Intermediaries Guidelines")

These Rules specify the obligations of intermediaries to take down content under specified circumstances.

Code of Criminal Procedure, 1973

This is the principal law governing criminal procedure in India, and which authorises courts and law enforcement agencies to demand the production of documents or other information in the course of an investigation.

2. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

2.1 Legislation

Under Section 5(2) of the ITA Act read with Rule 419-A (I) of the Indian Telegraph Rules, 1951 (ITR), either the Secretary to the Ministry of Home Affairs (in the case of the central government) or the Secretary to the Home Department (in case of the state government or union territory) or a person above the rank of Joint Secretary (in unavoidable circumstances) authorised by the respective government, during a public emergency or in the interests of public safety, may issue a written order directing an interception, if the official in question believes that it is necessary to do so in the: (a) interest of sovereignty and integrity of India; (b) the security of the State; (c) friendly relations with foreign states; (d) public order; or (e) the prevention of incitement of offences.

In case of an emergency, the prior approval of the aforementioned government officials may be dispensed with. In such a case, the interception or monitoring will have to be carried out by an officer not below the level of the Inspector General of Police.

Section 69 of the IT Act permits authorised government officials to intercept or monitor information transmitted, generated, received or stored in any computer. Accordingly, the service provider is required to extend all technical facilities, equipment and technical assistance to the authorised government officials to intercept the information and to provide information stored in the computer. The Interception Rules lay down the procedure to be followed by the government to authorise such interception or monitoring.

Under Section 69 of the IT Act read with Rule 3 of the Interception Rules, either the Secretary to the Ministry of Home Affairs (in the case of the central government) or the Secretary to the Home Department (in the case of the state government) or a person above the rank of Joint Secretary authorised by the relevant government department (in unavoidable circumstances), may issue an order for the interception of any electronic information transmitted, stored or generated over any computer, if the official in question believes that it is necessary to do so in: (a) the interest of sovereignty and integrity of India; (b) the security of the State; (c) friendly relations with foreign states; (d) public order; or (e) the prevention of incitement of offences.

The UASL, UL and the ISP License require the licensee to implement the necessary facilities and equipment for interception purposes in terms of the following provisions:

1) Clause 39.23 (xvi) of Part-I of the UL, Clause 41.20 (xvi) of the UASL and Clause 34.28 (xvi) of the ISP License require the licensee to ensure that the necessary hardware/software in their equipment is available for the carrying out of the lawful interception and monitoring from a centralised location.

2) Under Clause 23.2 of Part-I of the UL, Clause 41.7 of the UASL, and Clause 34.4 of the ISP License the licensee is required to install the equipment that may be prescribed by the government for monitoring purposes.

3) As per Clause 39.23 (xiv) of Part-I of the UL, Clause 34.28(xiv) of the ISP License and Clause 41.20 (xiv) of the UASL, in case of remote access of information, the licensee is required to install suitable technical devices enabling the creation of a mirror image of the remote access information for monitoring purposes.

4) Clause 8.2 of Part-II, Chapter VIII of the UL, and Clause 41.10 of the UASL License requires the licensee to install the necessary hardware/software to enable the government to monitor simultaneous calls.

Under Rules 12 and 13 read with Rule 19 of the Interception Rules, once the interception order has been issued as per Rule 3 of the Interception Rules, an officer not below the rank of the Additional Superintendent of Police shall make a written request to the intermediary to provide all facilities and the necessary equipment for the interception of the information.

Section 2(w) of the IT Act defines intermediary to include 'telecom service providers, network service providers and internet service providers'.

2.2 Licenses

Until 2013, the UASL was entered into between a telecom service provider and the DoT for the provision of access services. Similarly, until 2013, the ISP License was entered into between an internet service provider and the DoT for the provision of internet services. Both these licenses were granted typically for a period of 20 years. Under the UL, the UASL and the ISP License, licensees are bound to take all steps and provide all facilities to enable the government to carry out interception of communications. Clause 40.2 of Part-I of the UL, Clause 42.2 of the UASL and Clause 35.5 of the ISP License provide that the licensee must provide the necessary interception facilities as required under Section 5 of the IT ACT.

Clause 8.2 of Part-II of the UL, Clause 41.10 of the UASL and Clause 34.6 of the ISP License provide that designated government officials shall have the right to monitor the telecommunication traffic at any technically feasible point. The licensee is required to make arrangements for simultaneous monitoring by the government.

Clause 7.2 and 7.3 of Part-II, Chapter IX of the UL, Clause 34.8 of the ISP License, requires each ISP to maintain a log of all connected users and the service that they are using. The ISP is also required to maintain every outward login. The logs and the copies of all the packets originating from the Customer Premises Equipment ("CPE") of the ISP must be available in real time to the government.

2.3 Central Monitoring System

The Central Monitoring System ("CMS") is an interception and monitoring project of the Government of India which was approved in 2011. There is no legislation authorising the setting up of the CMS. Minimal information is available through newspaper reports and Parliamentary Questions. The Minister of Communications and Information Technology of the Government of India confirmed in 2016 that the CMS was already operational in Delhi and Mumbai, and is being set up in phases.

CMS is intended to automate the process of the interception and monitoring in order to ensure that the Law Enforcement Agencies and the telecommunications and internet companies are not involved in the process of interception. Under the UASL with respect to the CMS, the licensee is required to provide the connectivity through dark fibre up to the nearest multi-protocol label switching network at its own cost. The UL also has provisions for the licensees to assist the government in centralised monitoring.

3. DISCLOSURE OF STORED COMMUNICATIONS DATA

3.1 Legislation

The Code of Criminal Procedure ("CrPC") empowers a court or police officer in charge of a police station to seek the production of any 'any document or other thing' if the officer believes that said document is necessary for the purposes of any investigation.

Section 69 of the IT Act permits authorised government officials to intercept or monitor information transmitted, generated, received or stored in any computer. Accordingly, the service provider is required to extend all technical facilities, equipment and technical assistance to the authorised government officials to intercept the information and to provide information stored in the computer.

3.2 Licenses

Under the UL, the UASL and the ISP License Agreement, the licensee is required to provide access to all call data records as well any other electronic communication. Under Clause 8.3 of Part-II, Chapter VIII of the UL, and Clause 41.10 of the UASL, the licensee is required to provide the call data records of all the calls handled by the licensee as and when required by the government.

Clause 38.2 of Part-I of the UL, and Clause 33.4 of the ISP License requires the licensee to provide the government with the required tracing facilities to trace messages or communications, when such information is required for investigation of a crime or for national security purposes.

Section 91 of the CrPC permit a court or officer in charge of a police station to issue a summons or written order respectively, requiring the production of "any document or other thing... necessary or desirable for the purposes of any investigation, inquiry, trial or proceeding".

Section 69 of the IT Act permits authorised government officials to "intercept or monitor information transmitted, generated, received or stored in any computer". Accordingly, the service provider is required to extend all technical facilities, equipment and technical assistance to the authorised government officials to intercept the information and to provide information stored in the computer.

Interception has been defined under Rule 2(l) of the Interception Rules to include the acquisition of "the contents of any information" through any means in so far as it enables the content of the information to be made available to a person other than the intended recipient.

4. NATIONAL SECURITY AND EMERGENCY POWERS

4.1 Legislation

Under Section 5(1) of the ITA Act, if there is a public emergency or in the interest of public safety, the government believes it is necessary, the government has the power to temporarily take possession of the 'telegraph' established and maintained or worked on by any person authorised under the IT Act.

4.2 Licenses

The government has the following special powers under the UASL and the ISP License:

1) Under Clause 39.16 of Part-I of the UL, Clause 41.13 of the UASL and Clause 10.5 of the ISP License; the government may "take over the service, equipment and networks of the licensee" in the event that such directions are issued in the public interest by the Government of India in the event of a national emergency, war, low-intensity conflict, or any other eventuality.

2) As per Clause 39.1 of Part-I of the UL, Clause 41.1 of the UASL and Clause 34.1 of the ISP License, the licensee must "provide necessary facilities depending upon the specific situation at the relevant time to the Government to counteract espionage, subversive act, sabotage or any other unlawful activity".

3) Under Clause 39.24 of Part-I of the UL, Clause 41.5 of the UASL and Clause 5.1 of the ISP License, the government may revise the license Clauses at any time if "considered necessary in the interest of national security and public interest".

4) In terms of Clause 39.15 of Part-I of the UL, Clause 41.11 of the UASL and Clause 34.9 of the ISP License, the government may, through appropriate notification, block the usage of mobile terminals in certain areas of the country. In such cases, the licensee must deny service in the specified areas within six hours of receiving the request.

5) Under Clause 39.23 (xviii) of Part-I of the UL, 41.20(xviii) of the UASL and Clause 34.28(xviii) of the ISP License, the government may restrict the licensee from operating in any sensitive area on national security grounds.

   In addition, Clause 33.7 of the ISP License and Clause 39.14 of the UL provide that the "use of the network for anti-national activities" (such as breaking into an Indian network) may be deemed sufficient reason to revoke the license, and will be considered an offence punishable under criminal law.

   The IT Act, the UASL and the ISP License do not prescribe the method and the instrument that the government may use in this regard.

5. OVERSIGHT OF THE USE OF POWERS

There is no judicial oversight over the interception process.

With respect to the review of the interception of telephonic communication under the IT Act and the ITR, a Review Committee has been established under Rule 419-A(16) of the ITR at both the central and the state level. As per the ITR, every order issued by the relevant government officials has to be sent to the Review Committee.

The Review Committee is required to meet once every two months and if the Review Committee is of the opinion that an interception order was not in accordance with the provisions of the IT Act and the ITR, it may set aside the interception order and also order the destruction of the information obtained through interception.

Rule 419-A (17) provides that in cases where the interception has been carried out in an emergency, the relevant government official has to be informed of such interception within three working days and the interception has to be confirmed within 7 working days, otherwise the interception will have to cease and the same message cannot be intercepted without the prior approval of Union or state Home Secretary.

A similar Review Committee has also been established under the Interception Rules. Rule 22 of the Interception Rules provides for the establishment of a Review Committee to examine the interception or monitoring directions. If the Review Committee is of the opinion that the interception or monitoring directions are not in accordance with Section 69 of the IT Act, then it may set aside the direction and also order the destruction of the information obtained through interception.

With respect to CMS there is no judicial oversight over the project. The Review process is the same as provided for under Rule 419-A of the ITR as described above.

6. CYBERSECURITY AND CYBERCRIME

6.1 IT Act

The IT Act, in conjunction with the Information Technology Rules 2000, governs all electronic transactions, electronic communications and any electronic storage of information. The Information Technology Amendment Act 2008 (the "ITAA") goes further, serving to specifically regulate technology-related cybercrimes, critical information infrastructure protection, data security and privacy protection.

Sections 65 - 67 and 72 of the IT Act (as amended by the ITAA) outline the penalties that may be imposed for cybercrimes as summarised below.

SECTION	Offence	Penalty
65	Tampering with computer source documents.	Imprisonment up to three years, or a fine up to 200,000 Indian Rupees, or both.
66	Computer-related offences such as damage to a computer and to a computer system.	Imprisonment up to three years or a fine of 500,000 Indian Rupees, or both.
66B	Dishonestly receiving stolen computer resource or communication device.	Imprisonment up to three years or a fine of 100,000 Indian Rupees, or both.
66C	Identity theft.	
66D	Cheating by impersonation by using computer resources.	
66E	Violation of privacy (relates to intentional capturing, publishing and transmission of visual images of private body areas of an individual without such individual's consent).	Imprisonment up to three years or a fine of 200,000 Indian Rupees, or both.
66F	Cyberterrorism.	Life imprisonment.
67	Publishing or transmitting obscene material in electronic form.	First conviction – imprisonment up to three years and a fine of 500,000 Indian Rupees. Second conviction - imprisonment up to five years and a fine of 1,000,000 Indian Rupees.
67A	Publishing or transmitting of material containing sexually explicit acts (including child pornography).	First conviction – imprisonment up to five years and a fine of 1,000,000 Indian Rupees Subsequent conviction - imprisonment up to seven years and a fine of 1,000,000 Indian Rupees
72	Breach of confidentiality and privacy (relates to unauthorised disclosure of confidential information by an individual who has secure access to such confidential information).	Imprisonment up to two years or a fine of 100,000 Indian Rupees, or both.

6.2 Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the "CERT-IN Rules")

The CERT-IN Rules prescribe the functions and responsibilities of the Indian Computer Emergency Response Team ("CERT-IN") which was instituted by the Indian Central Government. The rules also outline the procedure for cybersecurity incident reporting, incident response and information dissemination.

Under rule 12 (1) (a) of the CERT-IN Rules, an individual, organization or corporate entity affected by a cybersecurity incident may report that incident to the CERT-IN. Service providers, intermediaries, data centres and body corporates are required to report cyber security incidents to CERT-IN. However, where the type of cybersecurity incident includes one of the following, this option to report becomes obligatory:

(a) targeted scanning/probing of critical networks/systems;

(b) compromised critical systems/information;

(c) unauthorized access of IT systems/data;

(d) defacement of a website or intrusion into a website and unauthorized changes (such as inserting malicious code/ links to external websites etc.);

(e) malicious code attacks (such as spreading of viruses,

worms, Trojans, botnets or spyware);

(f) attacks on servers (such as databases, mail and DNS and network devices such as routers);

(g) identity theft, spoofing and phishing attacks;

(h) Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks;

(i) attacks on critical infrastructure, SCADA systems and wireless networks; or

(j) attacks on applications (such as e-governance, e-commerce etc.).

Under rule 12 (1) (a) of the CERT-IN Rules, reporting on the above types of cybersecurity crimes must be completed within a reasonable time of occurrence or noticing the incident, to ensure timely action and minimise the damage as quickly as possible. Under s. 70 (B)(7) of the IT Act, service providers, intermediaries, body corporates, data centres or persons who do not submit information with regard to cybersecurity incidents to CERT-IN, can be prosecuted with imprisonment of up to 1 year.

6.3 Intermediaries Guidelines

The Intermediaries Guidelines relate to legal persons who (for themselves or on behalf of others) receive, store or transmit electronic records or provide any services with respect to such records i.e. internet and telecommunication companies acting as 'intermediaries'. These guidelines impose more onerous obligations upon intermediaries to report cybersecurity incidents and share information related to cybersecurity incidents with the CERT-IN.

6.4 Unified License Agreement

The Unified License Agreement requires telecommunication companies to create facilities to monitor all intrusions, attacks and fraud on its technical facilities and provide reports on the same to the DoT.

Law stated as of 21 February 2017

MALAYSIA – 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 Malaysian law..

1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

Legislation which specifically provides authority to intercept communications is summarised below. Where not explicit, these rights can be interpreted widely to require network operators and service providers to assist law enforcement and intelligence agencies in their surveillance and censorship activities.

1.1 Criminal Procedure Code (the "CPC")

Under section 116B, a police officer conducting a search under the CPC is to be given access to computerized data whether stored in a computer or otherwise. For the purpose of this section, "access" includes being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of the computerized data.

Section 116C gives the law enforcement agencies very wide powers to intercept communications which may be evidence related to an offence.

Under section 116C, the Public Prosecutor (the Attorney General, the Solicitor General in certain circumstances or the Deputy Public Prosecutor as may be appointed by the Public Prosecutor) may authorise a police officer to intercept any message transmitted or received by any communication, which may be evidence related to the commission of an offence. The CPC defines "offence" as any act or omission made punishable by any law for the time being in force, including offences such as money laundering or gambling. The Public Prosecutor may also require a communications service provider to intercept and retain a specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by that communications service provider, or authorise a police officer to enter any premises and to install on such premises any device for the interception and retention of a specified communication or communications of a specified description and to remove and retain such device.

Section 116C is silent as to whether a warrant is required, which will ultimately depend on the offence under investigation and the circumstances at hand. Under sections 62 and 116A, a search without warrant is possible if there is reasonable cause for suspecting that there is evidence of a security offence or concealed organised crime or any stolen property is concealed in any place and there are good grounds to believe that a delayed search is likely to result in their removal. A "security offence" has the same meaning as under the Security Offences (Special Measures) Act 2012 (set out immediately below).

1.2 Security Offences (Special Measures) Act 2012 (the "SOSM")

Section 6 SOSM allows the Public Prosecutor (the Attorney General) and police officers to intercept all communications likely to contain any information relating to the commission of a security offence. A "security offence" is an offence stated in chapter VI (offences against the state) or chapter VIA (offences relating to terrorism) of the Penal Code. For example, activity detrimental to parliamentary democracy, sabotage, waging war against the Yang di-Pertuan Agong (the King of Malaysia) and committing terrorist acts.

Section 6(1) states that the Public Prosecutor may authorise any police officer or any other person to:

(a) intercept, detain and open any postal article in the course of transmission by post;

(b) intercept any message transmitted or received by any communication; or

(c) intercept or listen to any conversation by any communication,

if he considers that it is likely to contain any information relating to the commission of a security offence.

For the purposes of section 6, the term 'communication' means "a communication received or transmitted by post or a telegraphic, telephonic or other communication received or transmitted by electricity, magnetism or other means". This gives the police the power to intercept a wide range of communications, including electronic communications.

Under section 6(2) SOSM, a police officer not below the rank of Superintendent of Police may do any of the above without authorisation of the Public Prosecutor in urgent and sudden cases where immediate action is required leaving no time for deliberation. In practice, this may give police the power to intercept communications in a wide range of circumstances, including electronic communications.

1.3 Communications and Multimedia Act 1998 (the "CMA")

There are a wide range of offences provided for under the CMA, including breach of licence conditions and telecommunication-specific issues such as improper or fraudulent use of network facilities/services.

Section 252 CMA allows an authorised officer or a police officer of or above the rank of Superintendent to intercept or to listen to any communication if a public prosecutor considers a communication is likely to contain information relevant to an investigation into an offence under the CMA or its subsidiary legislation.

The CMA defines "authorised officer" as any public officer or officer appointed by the MCMC and authorised in writing by the Minister with responsibility for communication and multimedia (presently the Minister of Communications and Multimedia (the "Minister")). "Intercept" is defined as the aural or other acquisition of the contents of any communications through the use of any electronic, mechanical, or other equipment, device or apparatus. "Communications" is defined as any communication, whether between persons, objects, or persons and objects, in the form of sound, data, text, visual images, signals or any other form or any combination of those forms.

Furthermore, section 265 CMA gives the Minister the right to require implementation of authorised interception capabilities by a licensee or class of licensees. A "licensee" is a person who either holds an individual licence or undertakes activities which are subject to a class licence. There are four categories of license that govern the relevant licensable activities: Network Facilities Service Provider; Network Service Providers; Applications Service Provider; and Content Applications Service Provider. A telecommunications service provider must be licensed if it is providing licensable activities.

Please note that section 265 is silent as to whether the implementation of the authorised interception capability would only be for purposes pursuant to a CMA offence. As a result, if it were to be read widely, it may cover offences outside of the CMA.

Section 38 gives the Minister the power to suspend or cancel an individual licence by declaration in certain circumstances, for example, if the licensee has failed to comply with the CMA or the conditions of its individual licence or the suspension or cancellation is in the public interest. Section 48 also provides similar cancellation powers to the Minister in respect of a class licensee.

Section 254 gives an authorised officer additional powers for the purposes of the execution of the CMA or its subsidiary legislation for specified purposes, including:

(a) to require the production of records, accounts, computerised data and documents kept by a licensee or other person and to inspect, examine and to download from them, make copies of them or take extracts from them; and

(b) to make such inquiry as may be necessary to ascertain whether the CMA and its subsidiary legislation have been complied with.

1.4 Copyright Act 1987 (the "Copyright Act")

Offences under the Copyright Act include: making for sale or hiring any infringing copy, distributing infringing copies, and circumvention of technological protection measures.

Under section 50B of the Copyright Act, the Public Prosecutor (the Attorney General) may authorise an Assistant Controller or a police officer not below the rank of Inspector Officer to intercept or to listen to any communications for the purpose of any investigation into an offence under the Copyright Act or its subsidiary legislation if he considers that the communication is likely to contain information relevant to the investigation.

An Assistant Controller comes under the purview of the Intellectual Property Corporation of Malaysia (the "MYIPO"), and is appointed or deemed to be appointed by the Director General of the MYIPO under section 5 Copyright Act.

Section 43H Copyright Act provides a copyright owner whose right has been infringed to notify (in the manner determined by the Minister charged with the responsibility for intellectual property at the relevant time) a service provider to remove or disable access to the electronic copy on the service provider's network within 48 hours of receipt of notification, although it is possible for a counter-notification to be issued by the person whose electronic copy of the work was removed or to which access has been disabled to require the service provider to restore the electronic copy or access to it within 10 business days, subject to further notification from the copyright owner.

1.5 Malaysian Anti-Corruption Commission Act 2009 (the "MACC")

Under section 43 MACC, if the Public Prosecutor (the Attorney

General) or an officer of the Malaysian Anti-Corruption Commission (the "Commission") of the rank of Commissioner or above, as authorised by the Public Prosecutor, considers that it is likely to contain any information which is relevant for the purpose of an investigation into an offence under the MACC, it may authorise any officer of the Commission to intercept any message transmitted or received by any telecommunication, or to intercept, listen to and record any conversation by any telecommunication, and listen to the recording of the intercepted conversation.

Section 47 also imposes a legal obligation on every person to give information if required by an officer of the Commission or a police officer on any subject which it is such officer's duty to inquire into under the MACC and which is in that person's power to give.

1.6 Certain interception powers are also authorised to particular law enforcement and intelligence agencies under the Kidnapping Act 1961, the Strategic Trade Act 2010, the Dangerous Drugs Act 1952, and the Dangerous Drugs (Forfeiture of Property) Act 1988.

2. DISCLOSURE OF COMMUNICATIONS DATA

As established above, various statutes provide wide powers of access, information gathering, search and seizure to law enforcement and intelligence agencies, which do not specifically distinguish between metadata and other types of data relating to communications, but may entail disclosure of such information. The following statutes give the relevant authorities wide powers of search and seizure that may include the right to access communications stored on a computer server. However, this is not an exhaustive list of the access rights given to law enforcement officers under Malaysian law. Many other statutory sources grant rights of search and seizure where there has been a breach of the relevant legislation, and information access rights given to law enforcement authorities are generally in relation to a commission or suspected commission of a crime or contravention of particular laws. Depending on the circumstances surrounding the request (i.e. if there is an offence being investigated), access rights may be wide, including entering premises by force and access to any data (including computerized data) as well as a right to intercept communications. Industry-specific regulators may also have inspection and audit requirements.

2.1 Computer Crimes Act 1997 (the "CCA")

The CCA generally protects against the misuse of computers, for example, hacking (see below for further information on the offences). The CCA also provides wide powers of search, seizure and arrest to a police officer of or above the rank of Inspector. Under section 10, whenever there is reasonable cause to believe that in any premises there is evidence of the commission of an offence under the CCA, an officer may be empowered to enter the premises, by force if necessary, and there to search for, seize and detain any such evidence and he shall be entitled to:

(a) have access to any program or data held in any computer, or have access to, inspect or check the operation of, any computer and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offence under the CCA;

(b) require (i) the person by whom or on whose behalf the police officer has reasonable cause to suspect the computer is or has been so used; or (ii) any person having charge of or otherwise concerned with the operation of, the computer, apparatus or material, to provide him with such reasonable assistance as he may require; and

(c) require any information contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible.

Section 10(3) of the CCA also states that any police officer may arrest without a warrant any person whom he reasonably believes to have committed or to be committing an offence against the Act. Section 11 of the CCA makes it an offence to obstruct a search when a police officer or authorised officer is executing any duty imposed or conferred by law. If there is a court order or search warrant, the network operators and service providers may be liable for contempt of court if they refuse to assist.

2.2 Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (the "AMLA")

Section 31 AMLA confers wide powers on an investigating officer to conduct a search without a warrant if the officer is satisfied or has reason to suspect that a person has committed an offence under AMLA. These powers include searching for any property, record, report or document, and inspecting and taking possession of or making copies of or taking extracts from any record, report or document so seized and detained, and detaining them for such period as he deems necessary.

Section 37 requires any person to deliver any property, document or information which an investigating officer has reason to suspect:

(a) has been used in the commission of an offence under AMLA: or

(b) is able to assist in the investigation of an offence under AMLA

that is in the possession or custody of, or under the control of, that person or is within the power of that person to furnish.

Under section 67(1), similar powers exist where the competent authority or an enforcement agency has reason to believe that a person is committing, has committed or is about to commit an offence under AMLA.

The definition of "document" for these purposes is very wide

and may be interpreted to include metadata relating to electronic communications.

2.3 Anti-Trafficking In Persons Act and Anti-Smuggling of Migrants Act 2007 (the "ATPAASMA")

Section 32 ATPAASMA stipulates that any enforcement officer conducting a search under ATPAASMA shall be given access to computerized data, whether stored in a computer or otherwise. For this purpose, the enforcement officer shall be provided with the necessary password, encryption code, decryption code, software or hardware or any other means required for his access to enable comprehension of the computerized data.

2.4 Communications and Multimedia Act 1998 (the "CMA")

The CMA gives the MCMC information gathering powers. Section 73 gives the MCMC the right to direct any person to provide them with information if the MCMC has reason to believe that the person has any information or document relevant to the performance of MCMC's powers and functions or is capable of giving any evidence which MCMC has reason to believe is relevant to the performance of its powers and functions.

Under section 77, MCMC may take and retain, for as long as necessary, any document provided to it pursuant to its information-gathering powers.

Under section 247, a magistrate may issue a warrant authorising any police officer not below the rank of Inspector or authorised officer to enter premises if it appears to the magistrate that there is reasonable cause to believe an offence under the CMA or its subsidiary legislation is being or has been committed on the premises or that those premises contain any evidence or thing which is necessary to an investigation. The authorised officer may enter the premises at a reasonable time with or without assistance, and if need be by force, and search for and seize any such evidence or thing. Section 247(8) states that if a search under section 247 indicates that there is any interference-causing equipment, radio apparatus or radiosensitive equipment, the authorised officer may direct that necessary steps be taken to ensure an interference-free environment.

Section 249 CMA gives the police officer and authorised officer conducting a search under the CMA (whether with or without a warrant) access to computerised data, however stored. "Access" is defined to include being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to comprehend computerised data, including access as defined under the CCA which provides the police with a wide range of rights in relation to accessing data.

Section 253 CMA makes it an offence to obstruct a search when a police officer or authorised officer is executing any duty imposed or conferred by law. The penalty for this offence is a fine not exceeding RM20,000.00 or imprisonment for a term not exceeding 6 months or both. If there is a court order or search warrant, the network operators and service providers may be liable for contempt of court if they refuse to assist.

2.5 General Consumer Code of Practice for the Communications and Multimedia. Industry (the "GCC")

The GCC requires a service provider, wherever possible to retain records of a customer's bill for a minimum period of one year. Material collected and recorded in relation to complaints handling processes is also to be retained by network operators and service providers for one year following the resolution of a complaint. However, the GCC also states that consumer data or information collected by service providers should not be kept longer than necessary.

The definition of "consumer" under GCC means a person who receives, acquires, uses or subscribes to services relating to communications and multimedia within the meaning of the CMA.

3. NATIONAL SECURITY AND EMERGENCY POWERS

Law enforcement and intelligence agencies have a number of special powers in times of emergency or for other special reasons. Below, we identify the common legislation invoked in such circumstances. Please note that there may be instances where emergency legislation is passed which is specific to a particular state within Malaysia. This is beyond the scope of this report.

3.1 Communications and Multimedia Act 1998 (the "CMA")

Under the CMA, a licensee shall, upon written request by the MCMC or any other authority, assist MCMC or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence or otherwise in enforcing the laws, including the protection of the public revenue and preservation of national security.

Under section 266, on the occurrence of any public emergency or in the interest of public safety, the Yang di-Pertuan Agong (the King of Malaysia) or the authorised Minister may:

(a) suspend the licence of any licensee, take temporary control of any network facilities, network service, applications service and/or content applications service owned or provided by a licensee in any manner as he deems fit;

(b) withdraw either totally or partially the use of any network facilities, network service, applications service and/or content applications service from any licensee, person or the general public;

(c) order that any communication or class of communications to or from any licensee, person or the general public relating to any specified subject shall not be communicated or shall be intercepted or detained, or that any such communication or its records shall be disclosed to an authorised officer mentioned in the order; or

(d) order the taking of possession of any customer equipment.

Under section 266(c), on the occurrence of any public emergency or in the interest of public safety, the Yang di-Pertuan Agong or the authorised Minister may order that any communication or class of communications to or from any licensee, person or the general public relating to any specified subject shall not be communicated or shall be intercepted or detained, or that any such communication or its records shall be disclosed to an authorised officer mentioned in the order.

3.2 Emergency (Essential Powers) Act 1979 (the "EEPA")

Section 2 EEPA gives the Yang di-Pertuan Agong the power to make any regulations whatsoever (the "Essential Regulations") which he considers desirable or expedient for securing public safety, the defence of Malaysia, the maintenance of public order and of supplies and services essential to the life of the community.

The Essential Regulations may, among other things, authorise the taking possession, control, forfeiture or disposal, on behalf of the Government of Malaysia, of any property or undertaking; or the acquisition, on behalf of the Government of Malaysia, of any property other than land; or authorise the entering and search of any premises; or provide for any other matter in respect of which it is in the opinion of the Yang di-Pertuan Agong desirable in the public interest that regulations should be made (sections 2(g), (h) and (o)).

3.3 Official Secrets Act 1972 (the "OSA")

Under section 6 OSA, any court may issue a search warrant to search for and seize a document, even though an offence under the OSA is not alleged, if it is satisfied that there is reasonable cause to believe a document contains matter or information prejudicial to the safety or interests of Malaysia and is directly or indirectly useful to a foreign power or to an enemy. "Document" is interpreted to include any other data embodied so as to be capable of being reproduced.

Section 12 OSA gives the Minister the power to require the production of certain messages sent to or from any place outside of Malaysia from any person who owns or controls any telecommunications device used for sending or receiving such messages (including the originals and transcripts of such messages and all other papers relating to the message). The request must be made by means of a warrant, and the messages should be provided to the Minister or any person named in the warrant.

There is also a duty under section 11 OSA to provide information when required to do so by the police, by any member of the armed forces or by an authorised public officer.

Sections 3(b) and (c) OSA stipulate that if, for any purpose prejudicial to the safety or interest of Malaysia, any person either makes any document or obtains, collects, records, publishes or communicates to another person any information which might be directly or indirectly useful to a foreign country, then they will be guilty of an offence punishable by life imprisonment. For the purpose of this section, "document" includes, in addition to a document in writing and part of a document:

(a) any map, plan, model, graph or drawing;

(b) any photograph;

(c) any disc, tape, sound track or other device in which sound or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and

(d) any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (as aforesaid) of being reproduced therefrom.

Under section 27 OSA, in the course of any court proceedings related to an offence under the OSA, an application may be made for a court order by the prosecution to exclude the public from any part of a hearing. The grounds required are that the publication of any evidence or statements made in the course of the proceedings would be prejudicial to the safety of Malaysia.

3.4 National Security Council Act 2016 ("NSCA")

Under the NSCA, the National Security Council ("Council") has the power, notwithstanding any other written law, to do all things necessary or expedient for or in connection with the performance of its functions including:

(a) to control and coordinate Government Entities on operations concerning national security; and

(b) to issue directives to any Government Entity on matters concerning national security.

Government Entity is defined to include:

(a) any ministry, department, office, agency, authority, commission, committee, board or council of the Federal Government, or of any of the State Governments, established under any written law or otherwise;

(b) any local authorities; and

(c) the Security Forces, defined as:

(i) the Royal Malaysia Police, the Royal Malaysia Police Volunteer Reserve and the Auxiliary Police referred to in the Police Act 1967;

(ii) the armed forces;

(iii) any force which is a visiting force for the purposes of Part 1 of the Visiting Forces Act 1960; or

(iv) the Malaysian Maritime Enforcement Agency established under the Malaysian Maritime Enforcement Agency Act 2004.

Under Section 18 of the NSCA, where the Council advises the Prime Minister that the security in any area in Malaysia is seriously disturbed or threatened by any person, matter or thing which causes or is likely to cause serious harm to the people, or serious harm to the territories, economy, national key infrastructure of Malaysia or any other interest of Malaysia, and requires immediate national response, the Prime Minister may, if he considers it to be necessary in the interest of national security, declare in writing the area as a security area. Upon a declaration being made under section 18, the Council may issue an executive order to the Director of Operations ("DO") or such Government Entities as the Council deems necessary in relation to the security area in the interest of national security. The DO has wide ranging powers in relation to security areas such as exclusion and evacuation of persons, establishing curfew and controlling movements of persons or any vehicle, aircraft or conveyance in and out of the security area.

Under Section 26, any member of the Security Forces may, without warrant and with or without assistance, stop and search any individual, vehicle, vessel, aircraft or conveyance in the security area if he suspects that any evidence of the commission of an offence against any written law is likely to be found and may seize any evidence so found. Under Section 34, any member of the Security Forces in a security area may use such force against persons and things as is reasonable and necessary in the circumstances to preserve national security.

Further, under Section 30(1), the DO or any person authorized by the DO may, if it appears to him to be necessary or expedient to do so in the interest of national security, or for the accommodation of any Security Forces, take temporary possession of any land, building or part of a building, or any movable property in any security area and may give such direction as appears to him necessary or expedient in connection with the taking of possession of that land, building or movable property.

Under Section 30(3), any land, building or movable property in temporary possession as per Section 30(1) above may be used for such purpose and in such manner by the DO or any person authorised by the DO as they think expedient in the interest of national security or for the accommodation of any Security Forces, notwithstanding any restriction imposed on the use thereof.

Section 17(2) of the NSCA also states that upon direction by the Council, any Government Entities or any person shall immediately make available any information or intelligence in its or his possession which relates to national security to the Council through the Director General. However, as the NSCA is a relatively new legislation, the scope and application of these sections have not yet been tested.

4. CENSORSHIP

4.1 Communications and Multimedia Act 1998 (the "CMA")

In general, the Minister and the MCMC are granted very wide powers to make determinations or declarations consistent with the objects and provisions of the CMA, the effect of which is that they may take control of or shut down network operators and service providers. Usually, the determinations or directives are issued pursuant to the CMA, which grants the Minister and the MCMC the power to issue determinations or directives on certain issues.

The CMA also contains several provisions regulating content and voluntary industry codes such as the Malaysian Communications and Multimedia Content Code (the "Code") (please see section 5.2 below) and General Consumer Code of Practice for the Communications and Multimedia Industry. While compliance with these voluntary industry codes by service providers is good practice but not mandatory, section 98 states that compliance with the voluntary code serves as a defence against any prosecution, action or proceeding of any nature taken against a person (who is subject to the voluntary industry code) regarding a matter dealt with in that code. It is also pertinent to point out that compliance with the General Consumer Code is part of the licence condition, and those who provide multimedia content may be required to comply with the Code. The MCMC may also direct any person to comply with both codes and failure to comply with such direction is an offence.

Section 211 of the CMA states that no content applications service provider shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person. Section 6 of the CMA defines content as any sound, text, still picture, moving picture, audio-visual or tactile representation, which can be manipulated, stored, retrieved or communicated electronically.

Under section 233, (a) a person who by means of any network facilities or network service or applications service knowingly makes, creates or solicits and initiates the transmission of obscene, indecent, false, menacing or offensive content with intent to annoy, abuse, threaten or harass any person; or (b) a person who knowingly by means of any network facilities or network service or applications service provides any obscene communication for commercial purposes or permits a network service or applications service under the person's control to be used for an activity described in (a), commits an offence.

Notwithstanding the above, Section 3 of the CMA, which states the objectives of the CMA provides that "nothing in the CMA shall be construed as permitting the censorship of the Internet".

4.2 Malaysian Communications and Multimedia Content Code (the "Code")

The Code provides guidelines and procedures for good practice in relation to the dissemination of online content to the public by service providers in the communications and the multimedia industry. The Code also regulates Internet Content Hosting Providers ("ICH") and Internet Access Service Providers.

Persons subject to the Code ("Code Subjects") who provide access to any electronic content (such as sounds, texts or pictures), but who do not control such content or have any knowledge of what it comprises, are deemed "innocent carriers". As such, they are not responsible for such content for the purposes of the Code. Nevertheless, this does not exempt them from the general measures in Part 6.0 of Part 5 where it expressly applies to them and, depending on the degree of control that Code Subjects may have over the online content, the specific measures in Parts 7.1 – 10.2 of Part 5 of the Code will have to be complied with (for example, to incorporate terms and conditions in their contracts such as the Code Subject's right to withdraw its hosting services where a user or subscriber contravenes Malaysian law).

The Code expressly states that ICHs are not required to do certain things, such as to block access by their users/subscribers to any material unless directed to do so by the Complaints Bureau, or monitor the activities of users and subscribers.

The Complaints Bureau is an arm of the Communications and Multimedia Consumer Forum, set up by the Malaysian Communications and Multimedia Commission to protect the rights of consumers in this sector. It deals with all complaints that relate to the Code.

4.3 Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (the "AMLA")

Section 6(3) stipulates that no person shall publish in writing or broadcast any information, including a report of any civil or criminal proceedings but excluding information published for statistical purposes by a competent authority or the Government, so as to reveal or suggest:

(a) that a disclosure was made under section 5; or

(b) the identity of any person as the person making the disclosure.

Section 5 relates to protection of informers and information relating to an offence under AMLA.

4.4 SEDITION ACT 1948

Section 10 states that where on the application of the Public Prosecutor it is shown to the satisfaction of a Sessions Court Judge that the making or circulation of a seditious publication:

(a) is or if commenced or continued would likely lead to bodily injury or damage to property;

(b) appears to be promoting feelings of ill will, hostility or hatred between different races or classes of the population of Malaysia; or

(c) appears to be promoting feelings of ill will, hostility or hatred between persons or groups of persons on the ground of religion,

the Sessions Court Judge shall make an order ("prohibition order") prohibiting the making or circulation of that seditious publication ("prohibited publication"). In relation to seditious publications by electronic means by a person who cannot be identified and which falls under any of the circumstances (a) to (c) above, the Sessions Court Judge shall make an order directing an officer authorized under the Communications and Multimedia Act 1998 to prevent access to such publication.

Subsection (1A) states that the prohibition order under subsection (1) shall:

(a) require every person having any copy of the prohibited publication in his possession, power, or control to deliver forthwith every such copy into the custody of the police; or

(b) in the case of a prohibited publication by electronic means:

(i) require the person making or circulating the prohibited publication to remove or cause to be removed wholly or partly the prohibited publication; and

(ii) prohibit the person making or circulating the prohibited publication from accessing any electronic device.

Bearing this in mind, some legal provisions may extend responsibility to network operators and service providers in relation to such laws even if the content is not actually provided or created by the network operators and service providers. These include abetting an offence punishable with imprisonment under section 116 of the Penal Code. In addition, under section 114A Evidence Act 1950, it is possible that the network operators and service providers may be presumed to be the publisher of the content contained on its customers' sites, unless the contrary is proved.

4.5 OTHER RELEVANT LEGISLATION

In relation to enforcement measures, under section 263 CMA, MCMC may request licensees to assist MCMC in preventing commission of an offence. This instruction may include blocking or removal of scam websites or websites with illegal content. Further, pursuant to section 51 CMA, MCMC may issue directions to "any person" regarding the compliance or non-compliance of the provisions of the CMA and its subsidiary legislations. This may include directions to comply or remedy non-compliance with provisions such as section 233 which sets out offences on improper use of network facilities or network services which appear to be wide enough to capture scam websites or websites with illegal content. MCMC largely works with the police and other law enforcement agencies to implement this, for example, through use of the Penal Code and sedition laws. The Penal Code, for example, provides for offences in relation to complaints about violent "hate" sites, including section 505 which makes it an offence to make, publish or circulate any statement, rumour or report:

(a) with intent to cause, or which is likely to cause, fear or alarm to the public, or to any section of the public whereby any person may be induced to commit an offence against the State or against the public tranquillity; or

(b) with intent to incite or which is likely to incite any class or community of persons to commit any offence against any other class or community of persons.

The penalty for an offence under this section is up to two years' imprisonment, a fine, or both.

The Penal Code also contains offences in relation to printing content containing slander or libel, and offences in relation to hosted sites which contain illegal content or encourage illegal acts.

5. OVERSIGHT OF THE USE OF POWERS

5.1 Communications and Multimedia Act 1998 (the "CMA")

Under the CMA, section 18 states that the Appeal Tribunal established under section 17 may review any matter on appeal, from a decision or direction of the MCMC, but not from a determination by the MCMC. Any decision by the Appeal Tribunal is final and binding on the parties to the appeal and is not subject to further appeal.

Section 120 provides that an aggrieved person or person whose interest is adversely affected by a decision or direction (but not a determination) of MCMC may appeal to the Appeal Tribunal for a review of the merits and the process of certain decisions or directions of the MCMC, unless the matter is not subject to an appeal to the Appeal Tribunal.

Section 121 provides for judicial review where a person is affected by a decision or other action of the Minister or MCMC and all other remedies provided under the CMA have been exhausted.

5.2 Security Offences (Special Measures) (Interception of Communications) Regulations 2012 under the SOSM (the "2012 Regulations")

Regulation 3 requires that a police officer who has acted under section 6(3) SOSM (interception without authorisation by the Public Prosecutor in urgent cases where immediate action is necessary) must submit a written report to the Public Prosecutor (the Attorney General) containing specified information detailed in the Second Schedule of the 2012 Regulations. The information required includes details of the officer making the interception, details relating to the individual whose communication was intercepted, the facts surrounding the investigation and the grounds for using interception.

5.3 Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (the "AMLA")

Section 31(4) requires the investigating officer, in the course of his investigation or search, to prepare and sign a list of all property, documents or information detained and state in the list the location in which or the person on whom, the property, document or information is found.

5.4 General power for Judicial Review ("JR")

Judicial review of the decision-making process of an authority exercising a power of a public nature by a court is available even if the executive/administrative decision is not open to any appeal or is expressed by the law to be 'final and conclusive'. Courts are not necessarily prevented from reviewing such acts or decisions.

The powers of the High Court in relation to JR are enshrined under the Specific Relief Act 1950 and the Courts of Judicature Act 1964. Grounds for JR include procedural impropriety, illegality, and irrationality in the decision-making process.

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

Restrictions on network operators and service providers

Under federal Malaysian law, there are no specific restrictions on publishing aggregate data relating to, for example, the volume of interceptions made in a single year. However, where not already set out in this report, the following laws could be employed to restrict such publication, in certain circumstances.

6.1 Communications and Multimedia Act 1998 (the "CMA")

The CMA provides confidentiality obligations in relation to documents or information considered to be confidential by the MCMC in the course of an investigation or trial or which relate to the affairs of the Appeal Tribunal (sections 26B, 61 and 63 CMA). MCMC may also issue a direction pursuant to section 51 CMA, requiring any persons including network operators or service providers to comply with such secrecy obligations. Such confidentiality obligations are open to judicial review under section 121.

In addition, under section 80 CMA, the MCMC is itself bound by certain obligations in respect of the publication of information. Section 80(3) CMA states that the MCMC must not publish any information disclosed to it if the publication would:

(a) disclose a matter of a confidential character;

(b) be likely to prejudice the fair trial of a person; or

(c) involve the unreasonable disclosure of personal information about any individual (including a deceased person).

However, the MCMC may publish an abstract relating to such information provided that the particulars in the abstract are not be arranged in any way which would compromise or prejudice the person providing such information.

Aggregate data published by government agencies.

6.2 Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (the "AMLA")

Section 6(3) AMLA (described in section 4.3 above) prevents the disclosure of certain information in legal proceedings, however, it exempts information published for statistical purposes by a competent authority or the government.

Generally, however, government agencies do not publish aggregate data in relation to the federal powers of interception, disclosure of data or censorship, as described in this report.

7. CYBERSECURITY

7.1 Communications and Multimedia Act 1998 ("the CMA")

The provisions under the CMA on cybersecurity are general. As such, the following sets out the general safeguards and remedies that may be used to ensure cybersecurity in Malaysia and should not be considered an exhaustive list.

Under Section 263 CMA, there is a general duty on licensees to use best endeavors to prevent their networks or services from being used in or in relation to the commission of any offence under Malaysian law.

The MCMC may direct a licensee or class of licensees to develop, in consultation with the authorities specified by the MCMC, a disaster plan for the survivability and recovery of any network facilities, network service, applications service or content applications service in case of a disaster, crisis or civil emergency as per Section 267.

There are also consumer codes and toolkits that have been prescribed in relation to cybersecurity. For example, there is the General Consumer Code ("the GCC"), which is a voluntary code issued by the Communications and Multimedia Consumer Forum of Malaysia ("the CFM"). The GCC states that service providers who create, maintain, use or disseminate individually identifiable information should take both appropriate measures to ensure its reliability and reasonable precautions to protect this type of information from loss, misuse or alteration. The GCC also states that service providers should take reasonable steps to ensure that third parties to whom they transfer such information are aware of these security practices, and take the same precautions to protect any such transferred information.

Security measures are also prescribed under the Internet Access Service Provider ("the IASP") Sub-Code issued under the GCC. The IASP Sub-Code states inter alia that service providers should have guidelines on how to implement security in their network and there must be some level of standard procedures to be followed. The code further states that the policy may cover items such as physical and environmental security, system access control and computer and network management. Moreover, it is important to note that whilst compliance with the GCC and the IASP Sub-Code is not mandatory, save for licensed service providers, the MCMC does have the power to direct any person to comply with the GCC. Any failure to comply with such direction constitutes an offence which would attract a fine of up to RM200,000.

Furthermore, failure to comply with any of the provisions of the CMA as described above may be considered a general offence which can incur liability of a fine not exceeding RM100,000 or 2 years' imprisonment or both, in addition to the forfeiture of anything seized.

"Determination" is defined in the CMA to mean "determinations made by MCMC under section 55 CMA" (which states that the MCMC may determine any matter specified in the CMA as being subject to MCMC's determination).

"Directions" are defined as directions issued by MCMC under section 51 CMA which provides that "The Commission may from time to time issue directions in writing to any person regarding the compliance or non-compliance of any licence conditions, and including but not limited to the remedy of a breach of a licence condition and the provisions of this Act or its subsidiary legislation."

Section 18 CMA provides that the Appeal Tribunal (which is established under Section 17) may review any decision or direction of the MCMC, but may not review any determination made by the MCMC. Therefore, under Section 120, an aggrieved individual whose interests have been adversely affected by a decision or direction (but not a determination) made by the MCMC may appeal to the Appeal Tribunal for a review of the merits of their case and the process taken by MCMC, unless the matter is not subject to an appeal to the Appeal Tribunal. Any decision that is made by the Appeal Tribunal is final and binding and not subject to further appeal. However under Section 121, an application for judicial review is available to an individual who is affected by a decision or other action of the Minister or MCMC where all other remedies provided under the CMA have been exhausted.

7.2 Personal Data Protection Act 2010 ("the PDPA")

The PDPA governs any processing of "personal data" completed in respect of a "commercial transaction" and applies if the "data user" (which is a concept equivalent to "data controller" in other jurisdictions) is:

(a) established in Malaysia and the personal data is processed by that person or any other person employed or engaged by that establishment; or

(b) not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia.

Whilst the security requirements under the PDPA are general, more specific requirements are imposed under the Personal Data Protection Standards 2015 ("the PDP Standards") as discussed below.

The Security Principle (as set out in the PDPA and expanded by the PDP Standards) requires the data user to take steps to protect any of the personal data processed from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction having regard to:

(a) the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;

(b) the place or location where the personal data is stored;

(c) any security measures incorporated into any equipment in which the personal data is stored;

(d) the measures taken to ensure the reliability, integrity and competency of personnel who have access to the personal data; and

(e) the measures taken to ensure the secure transfer of the personal data.

If the processing is carried out by a data processor on behalf of a data user, that data user is required for the purposes of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction to ensure that the data processor:

(a) provides sufficient guarantees in respect of the technical and organizational security measures governing the processing; and

(b) takes reasonable steps to ensure compliance with those measures.

There are also security requirements imposed under the Personal Data Protection Regulations 2013 ("the PDP Regulations"), which require data users to develop and implement a security policy for the purposes of the Security Principle described above. Such security policy must comply with the security standards set out from time to time by the Personal Data Protection Commissioner ("the Commissioner"). Data users must further ensure that the security standard, when processing the personal data, is complied with by any data processor that carries out the processing of the personal data on its behalf.

Additionally security standards can be found within the PDP Standards. The PDP Standards make recommendations for ensuring the security standard is maintained when dealing with personal data management, including suggestions such as that:

(a) the data user should have a backup/recovery system and the latest antivirus software to protect their clients data in the event of trespassing;

(b) the data user should be required to monitor the malware and scan the computer operating system with a schedule to prevent an attack on the electronically-kept data; and

(c) the electronic transfer of personal data should be restricted unless permitted (for related activity only) by the authorized officer.

It is the Commissioner who has the authority to carry out an inspection of:

(a) any personal data systems used by data users for the purpose of ascertaining information to assist the Commissioner in making recommendations to the relevant data user relating to the promotion of compliance with the provisions of the PDPA, in particular the Personal Data Protection Principles, by the relevant data user; and

(a) any personal data system used by data users belonging to a class of data users for the purpose of ascertaining information to assist the Commissioner in making recommendations to the class of data users to which the relevant data user belongs relating to the promotion of compliance with the provisions of this PDPA, in particular the Personal Data Protection Principles, by the class of data users to which the relevant data user belongs.

Non-compliance with the requirement to implement a security policy and to process personal data in accordance with any standards issued by the Commissioner may incur fines up to RM250,000 and/or two years' imprisonment. Also note that in certain circumstances companies' officers may also be found personally liable for offences under the PDPA in addition to the companies themselves.

The Commissioner, under the Ministry of Communications and Multimedia may, instead of convicting, serve an enforcement notice directing the data user to take certain steps to remedy any contraventions of the PDPA within a specified time period, and may order the cessation of the processing of personal data pending such remedy. However, failure to comply with an enforcement notice shall incur criminal liability in its own right.

Section 93 PDPA permits any person who is aggrieved by a decision of the Commissioner made in accordance with his authority under the PDPA to appeal the decision to the Appeal Tribunal. This section outlines in particular the appeal procedure to be used when appealing to the Appeal Tribunal in relation to a failure of the data user to comply with a data access or data correction request under Division 4 of Part II.

7.4 OTHER STATUTORY PROVISIONS

The section above does not cover the provisions of the Digital Signature Act 1997. It is also important to note that various other laws which are not specific to cybersecurity may also be applied in the context of cybersecurity, depending on the subject matter, such as theft, official secrets and national security offences.

8. CYBERCRIME

8.1 Computer Crimes Act 1997 (the "CCA")

The CCA generally protects against the misuse of computers, such as through hacking. The main offences discussed under the CCA and the penalties they attract are as follows:

CCA SECTION	Offence	Penalty
Section 3	Unauthorised access to computer material Described as causing a computer to perform any function with intent to secure access to any program or data held in any computer, the access of which the individual intends to secure is unauthorized and they are aware at the time when causing the computer to perform the function that this is the case.	A fine not exceeding RM50,000 or 5 years imprisonment or both.
Section 4	Unauthorized access with intent to commit or facilitate commission of further offence. Described as committing an offence referred to in Section 3 CCA (above) with intent: (i) to commit an offence involving fraud or dishonesty or which causes injury as defined in the Penal Code; or (ii) to facilitate the commission of such an offence whether by the offender or by any other person.	A fine not exceeding RM150,000 or imprisonment for a term not exceeding 10 years or both.
Section 5	**Unauthorised modification of the contents of any computer** Described as carrying out any act which an individual knows will cause unauthorized modification to the contents of any computer.	A fine not exceeding RM100,000 or imprisonment for a term not exceeding 7 years or to both. If the act is done with the intention of causing injury as defined in the Penal Code, the penalty is increased to a fine not exceeding RM150,000 and/or imprisonment for a term not exceeding 10 years.
Section 6	**Wrongful communication** Described as communicating directly or indirectly a number, code, password or other means of access to a computer to any person other than the person to whom the individual is duly authorized to communicate.	A fine not exceeding RM25,000 or imprisonment for a term not exceeding 3 years or both.

Note that the CCA shall, in relation to any person, whatever his nationality or citizenship, have effect outside as well as within Malaysia. Where an offence under the CCA is committed by any person in any place outside Malaysia, he may be dealt with in respect of such offence as if it was committed at any place within Malaysia. Moreover, the CCA shall apply if, for the offence in question, the computer, program 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 (s.9).

The only appeal mechanism available under the CCA is judicial review as discussed under cybersecurity above.

8.2 Communications and Multimedia Act 1998 (the "CMA")

Depending on the facts, the cybercrime in question may fall foul of several offences under the CMA. Some of the relevant offences and penalties that are dealt with under the CMA are as follows:

SECTION	Offence	Penalty
Section 231	Using any apparatus or device with the intent to obtain information regarding the contents, sender or addressee of any communication without an approval by a registered certifying agency.	A fine not exceeding RM50,000 or 2 years' imprisonment or both.
Section 233	Improper use of network facilities or network services. Described as where an individual, by means of any network facilities or network service or applications service knowingly makes, creates or solicits and initiates the transmission of, any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; or initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with the intent to annoy, abuse, threaten or harass any person at any number or electronic address or, where a person knowingly: (a) by means of a network service or applications service provides any obscene communication for commercial purposes to any person; or (a) permits a network service or applications service under the person's control to be used for an activity described in paragraph (a).	A fine not exceeding RM50,000 or to 1 year's imprisonment or both, and a further fine of RM1,000 for every day during which the offence continues after the conviction.
Section 234	Unlawfully intercepting, attempting to intercept, or procuring interception by any other person of any communications and/or disclosing or attempting to disclose the contents of any communications, knowing or having reason to believe that the information was obtained through interception in contravention of the CMA, or using or attempting to use such contents.	A fine not exceeding RM50,000 or 1 year's imprisonment or both.
Section 235	Any willful, dishonest or negligent act or omission, to extend, tamper with, adjust, alter, remove, destroy or damage any network facilities or any part of them.	A fine not exceeding RM300,000 or to 3 years' imprisonment or both.
Section 236	Offences in relation to counterfeit access devices, unauthorized access devices and device-making equipment, with knowledge or intention to defraud. Note in particular Section 236(1)(d) which makes it an offence for a person, who knowingly or with intention to defraud, possesses, produces, assembles, uses, imports, sells, supplies or lets for hire, or has control or custody of any modified or altered equipment, device or apparatus or any hardware or software used for such modification or alteration, used to obtain unauthorized use of any network service, applications service or content applications service.	A fine not exceeding RM500,000 or 5 years' imprisonment or both.

Note that the CMA applies both within and outside Malaysia. As such, the CMA shall apply to any person beyond the geographical limits of Malaysia and her territorial waters if such person is a licensee under the CMA or provides relevant facilities or services under the CMA in a place within Malaysia.

Again, the only appeal mechanism available under the CCA is judicial review as discussed under cybersecurity above.

8.3 Other laws

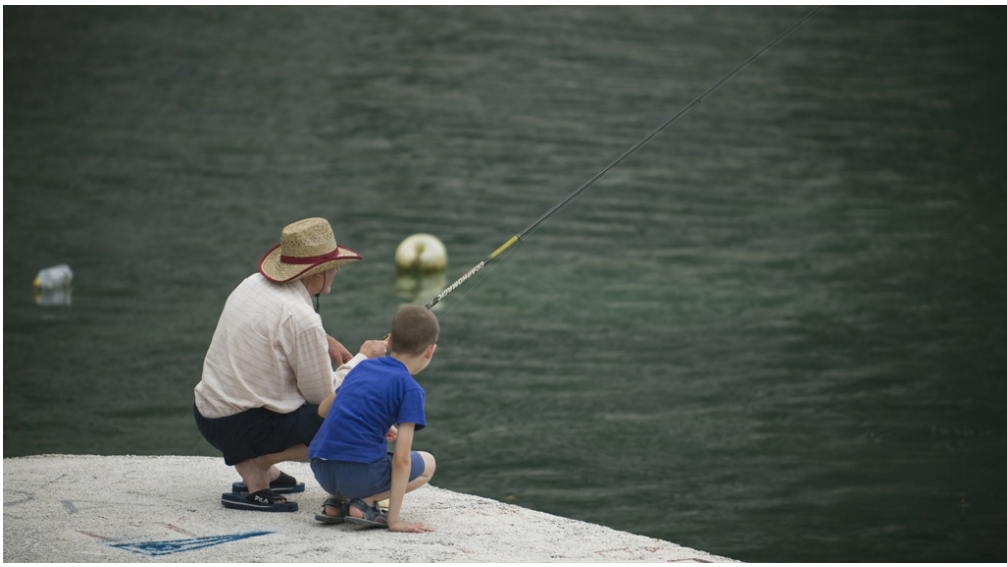
As for cybersecurity, various other laws which are not specific to cybercrime may also be applied in the context of a cybercrime offence, depending on the subject matter (such as theft, sedition, official secrets and national security offences).

Law stated as at 21 February 2017.

MONTENEGRO – 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 Montenegrin law.



1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

1.1 Constitution of Montenegro (Official Gazette of Montenegro no.1/2007 and 38/2013, Ustav Crne Gore) (the "Constitution")

Article 42 of the Constitution guarantees confidentiality of letters, telephone conversations and other means of communication and provides that derogation from this right is allowed only on the basis of a court decision if necessary in criminal proceedings or for the purposes of national security. These rights may only be limited by the law and pursuant to Article 24, for the purpose provided by the Constitution and to the extent necessary to satisfy the constitutional purpose of the limitation in question in an open and free democratic society.

1.2 Electronic Communications Act (Official Gazette of the Republic of Montenegro nos. 40/2013, 56/2013 and 2/2017, Zakon o elektronskim komunikacijama) (the "ECA")

Article 172 paragraph 2 ECA prohibits interception which includes listening, eavesdropping or keeping data regarding communication and its interruption or monitoring by another person, without the consent of the user of such communication. Rarely, the acts defined in Article 172 paragraph 2 may be carried out if they are necessary, adequate and proportionate in the interests of national security, defence, the prevention of crime, the investigation of a crime, to reveal and prosecute criminal offenders or to combat the unauthorised use of a system for electronic communications, to find or rescue people or for the protection of lives and property pursuant to Article 172 paragraph 4.

In accordance with Article 172 paragraph 4 ECA, an operator is obliged to provide, upon the request of the competent government agency and at their own expense, necessary technical and organizational conditions to enable the interception of communication and to prove to the Agency for Electronic Communication (the "Agency") that it had provided such conditions. An operator is also obliged under Article 180 to provide a permanent record of that measure, and to keep the collected data as an official secret in cooperation with the competent authority on whose request the interception is performed,.

The ECA does not impose an obligation on network operators and service providers to directly intercept individual customer communications, nor does it specify which government agencies are authorised to request such interception. The ECA also does not provide a maximum duration for an interception carried out. Interceptions are permitted under the Constitution for the purposes of conducting criminal proceedings or for the protection of national security. However, only the competent criminal court (whose order is implemented by the police) and the Agency for National Security (the "ANS") are authorised to require such interception under the conditions stipulated in the ECA and the legislation concerning their activities. The maximum duration for each interception is regulated by the specific legislation applicable to the activities of the criminal courts and the ANS.

1.3 Criminal Procedure Code (Official Gazette of Montenegro nos. 57/2009, 49/2010, 47/2014, 2/2015, 35/2015 and 58/2015, Zakonik o krivičnom postupku) (the "CPC")

Under the CPC, the interception and surveillance of electronic communications is stated to be a secret surveillance measure available both at the pre-investigation stage and the investigation stage of criminal proceedings. Under Article 157, such measures may be ordered against a person suspected of committing or preparing certain categories of crimes if

evidence of that crime cannot be collected in any other way, or if gathering of evidence by other means would cause disproportional risk or jeopardize lives. The relevant crimes for this purpose are those punishable by imprisonment of 10 years or more, organized crime, certain specifically listed crimes, such as money laundering and blackmail, cybercrime and bankruptcy crimes punishable with imprisonment of 8 years or more as per Article 158.

According to Article 157, interception may also be ordered against a person who is reasonably suspected of transferring messages to and from an individual suspected of committing one of the crimes outlined above, or whose phone or other means of communication has been used by a suspect. The order for such interception is issued by the competent criminal court upon the written request of the State Prosecutor for a maximum period of four months, with the possibility of an extension of up to 18 months as per Article 159. The court's order must be accompanied with a separate order containing the phone number or email address of the suspect to be intercepted and the duration of the interception which will be implemented by the police, to whom the network operator or service providers shall provide all necessary assistance pursuant to Articles 159 and 160.

Exceptionally, if written approval cannot be issued in time and any delay would be detrimental to the investigation, interception may be commenced based on the oral approval of the investigation judge or the State Prosecutor. In this case, a written order for interception must be issued within 12 hours of obtaining oral approval as per Article 159. Under Article 159 and Article 160, network operators and service providers are obliged to enable the interception of communications by authorised police officers. If the State Prosecutor decides not to initiate criminal proceedings against the suspect, the collected materials must be delivered to the investigation judge for destruction under Article 160. Pursuant to Article 161, evidence collected by interception which was not ordered or performed in accordance with this procedure will be declared inadmissible and the competent court shall order their destruction.

1.4 The Agency for National Security Act (Official Gazette of Montenegro, nos. 28/2005, 86/2009, 73-2010, 20/2011 and 8/2015 Zakon o Agenciji za nacionalnu bezbjednost) (the "ANSA")

The ANSA authorises the ANS to collect data by secret interception and surveillance of electronic communications if other investigation measures would not be expected to provide an adequate result or if it would cause disproportionate risk or threaten lives or health as per Articles 9 and 13.

Article 14 states that when there is a reasonable suspicion of a threat to national security, an interception may be ordered by the decision of the President of the Supreme Court of Montenegro, or in his/her absence the designated judge of that court.

Such interception is ordered for a period of three months and for serious reasons may be extended for additional three month periods. However under Article 15, the interception's overall duration must not exceed 24 months. Article 15 also provides that network operators and service providers are obliged to enable and guarantee conditions necessary for such interception.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Electronic Communications Act (Official Gazette of Montenegro nos. 40/2013, 56/2013 and 2/2017, Zakon o elektronskim komunikacijama) (the "ECA")

Network operators and service providers are obliged to retain certain data on traffic and location, as well as data relevant for the identification and registration of their customers. Such data may only be retained for the purposes of national security, defence, the prevention of crime, to investigate, reveal and prosecute criminal offenders or for the unauthorised use of a system for electronic communications. It may also be used pursuant to Article 181 to find or rescue people or for the protection of lives and property.

Under Article 181, network operators and service providers must also provide, at their own expense, necessary technical and organizational conditions which would enable competent government agencies to take over such data. This would oblige a network operator or service provider to decrypt encrypted data when required to do so by a court order.

According to Article 181 paragraph 5, the period of retention must not be shorter than six months nor longer than two years from the moment the communication occurred. Note however that government agencies may request access to the metadata retained by network operators and service providers. Network operators and service providers are obliged to keep annual records and statistics on data which have been delivered to government agencies and records on requests for the delivery of retained metadata which could not be executed under Article 181 paragraph 6.

According to Article 182, network operators and service providers are obliged to retain data on:

(a) tracing and identifying the source and destination of a communication;

(b) identifying the location of the parties to the communication;

(c) determining the date, time and duration of a communication;

(d) identifying the type of communication;

(e) identifying users' terminal equipment; and

(f) identifying the location of the users' mobile terminal equipment.

Under the provisions of Article 181 paragraph 3, network operators and service providers must not retain the content of

customer communications. However, since Article 180 paragraph 2 allows interception of electronic communications on the basis of a court decision, if such a court decision contains an order for the retention of the content of electronic communications, the network operators and service providers would be obliged to act upon it.

Article 183 paragraph 1 further obliges network operators and service providers to ensure that the quality and level of protection of retained metadata is the same as the quality and level of protection of the data circulating on the network. In addition, operators should undertake adequate technical and organizational measures to prevent unlawful or accidental destruction, loss or modification of retained metadata and the unauthorised storage, processing, access or disclosure of the retained metadata. Access to the retained metadata should only be granted to those persons authorised by the network operator or service provider. Any metadata not accessed at the end of a prescribed period of retention must be destroyed.

2.2 Criminal Procedure Code (Official Gazette of Montenegro nos. 57/2009, 49/2010, 47/2014, 2/2015, 35/2015 and 58/2015, Zakonik o krivičnom postupku) (the "CPC")

Under the CPC, if there is a reasonable suspicion that a prosecutable offence has been committed by the registered owner or user of a telecommunication device, the police may, based on the order of the investigation judge, request from the operators of the telecommunication services verification of the identity, duration and frequency of communication with certain electronic communication addresses, the location of the person who is being communicated, as well as the identification of the device. The police may also identify via technical devices the international identification number of the user (IMSI number), the international mobile equipment identification number (IMEI number) and the location of telephones and other means of electronic communication. The police may also make such requests with respect to a person connected to the registered owner or user of a telecommunication device.

The order of the investigation judge must be accompanied with a separate order containing the phone number, email address, IMSI number, IMEI and IP address of the suspect.

Exceptionally, if written approval cannot be issued in time and any delay would be detrimental to the investigation, the collection of metadata may commence based on the oral approval of the investigation judge. In such a case, a written order for the interception must be issued within 24 hours of obtaining oral approval. If the State Prosecutor decides not to initiate criminal proceedings against the suspect, the collected materials must be delivered to the investigation judge for destruction. Metadata collected contrary to this procedure will be declared inadmissible under Article 257a and the competent court shall order its destruction.

2.3 Police Act (Official Gazette of Montenegro nos. 44/2012, 36/2013 and 1/2015, Zakon o unutrašnjim poslovima) (the "PA")

Under the PA, the police is authorized to collect personal and other data to the extent necessary for the performance of their activities aimed at the prevention and suppression of crimes and protection of public order under Article 37 PA. State bodies, local authorities and legal entities are obliged to enable inspection and to deliver it at the request of the police data from their records.

A request made by the police to collect such data must contain the following:

(a) the legal grounds for the collection of the data;

(b) the details of the requested data;

(c) the purpose for which the data is requested;

(d) sufficient information necessary for determining the identity of the person to whom the requested data is related to; and

(e) a warning that it is a criminal offence to reveal to any third party the content of the request or what data is provided under it.

The police may also electronically inspect the records kept by legal entities if the entity has the technical arrangements to allow electronic inspection.

Note however under Article 39, if the data is requested:

(a) for the purpose of commencing or continuing a criminal investigation - the police is not obliged to state in the written request why the criminal investigation is starting or continuing; and

(a) based on a court order or state prosecutor`s order - the police do not have an obligation to explain why the data is being requested.

2.4 The Agency for National Security Act (Official Gazette of Montenegro, nos. 28/2005, 86/2009, 73/2010, 20/2011 and 8/2015, Zakon o Agenciji za nacionalnu bezbjednost) (the "ANSA")

On the basis of a court decision, the ANS is authorised to collect data by the secret interception and surveillance of electronic communications which encompasses the content of the electronic communication, communication data (data on traffic, unsuccessful attempts to establish the communication and data on location of a user of an electronic communication), if other investigation measures would not be expected to provide an adequate result or if they would cause a disproportionate risk or threaten people's lives or health as per Articles 9 and 13. On the written request of the ANS, network operators and service providers are required pursuant to Article 8 to enable access to the data contained in their records and to keep all such requests a secret.

Moreover, according to Article 15, operators and service providers are obliged to enable and guarantee the conditions for performance of such surveillance.

3. NATIONAL SECURITY AND EMERGENCY POWERS

3. Defence Act (Official Gazette of Montenegro, nos. 47/2007, 86/2009, 88/2009, 25/2010, 40/2011, 14/2012 and 2/2017, Zakon o odbrani) ("DA")

In a "state of emergency", defined as a natural disaster, a technology or environmental disaster, an epidemic, a danger to the public security or a threat to the constitutional order according to Article 5 paragraph 1, subparagraph 6 or a "state of war", defined as the state of imminent war, danger or military attack on the territory of Montenegro under Article 5 paragraph 1, subparagraph 7, legal entities in the field of postal-telegraph-telephone traffic and other carriers of telecommunications systems must prioritise the delivery of the services as specified by the Ministry of Defence pursuant to Article 21 paragraph 1.

3.2 Electronic Communications Act (Official Gazette of Montenegro nos. 40/2013, 56/2013 and 2/2017, Zakon o elektronskim komunikacijama) (the "ECA")

Paragraphs 1 and 3 of Article 61 obliges network operators and service providers to prepare an action plan for the protection of the integrity of electronic communications networks and their usage in a state of emergency or war and to submit this plan to the Ministry of Information Society and Telecommunications, the Agency for Electronic Communications, any other competent state bodies in charge of defence and security and the administrative body in charge of inspection control.

In cases of emergency, network operators and service providers are obliged to make available their electronic communications networks to the competent state bodies as per Article 61 paragraph 4, and to provide prioritised communication between certain terminal points which are defined by the government. For the purpose of enabling such prioritised communication, the government may order a network operator or service provider to temporarily disable its other network connections or to undertake other measures, if it deems it necessary pursuant to Article 62.

3.3 Constitution of Montenegro (Official Gazette of Montenegro no.1/2007 and 78/2013, Ustav Crne Gore) (the "Constitution")

Article 25 provides that in a state of emergency or a state of war, the Constitution allows the introduction of measures which derogate from the overarching principle of confidentiality of letters, telephone conversations and other means of communication and the protection of personal data. Consequently, in such instances government agencies may request access to customer communications data and/or their networks held by the network operators and service providers, without following the usual procedure of presenting a court decision authorising the interception or access to retained data. According to Article 132 and 133, a state of war or emergency is proclaimed by the Parliament or by the Council for the Security and Defence if the Parliament is not in position to convene.

4. CENSORSHIP

4.1 Enforcement and Security Act (Official Gazette of Montenegro, no. 36/2011, 28/2014 and 20/2015 Zakon o izvršenju i obezbeđenju) ("ESA")

Although there is no specific provision which explicitly regulates censorship or the blocking of IP addresses, network operators and service providers would be obliged to censor customer communications pursuant to the ESA, if such an order were given by a competent court in the form of an interim measure or in the form of a final court decision.

5. OVERSIGHT OF THE USE OF POWERS

5.1 Judicial Oversight

Since the CPC and ANSA provide that interception of electronic communications is allowed on the basis of a court order, each interception is overseen by the competent criminal court which ordered the interception and which monitors its enforcement as per Article 180 paragraph 2 ECA; Article 159 paragraphs 1 and 5 and Article 160 CPC; and Articles 14 and 15 ANSA.

5.2 Electronic Communications Act (Official Gazette of Montenegro nos. 40/2013, 56/2013 and 2/2017, Zakon o elektronskim komunikacijama) (the "ECA")

Although the ECA does not explicitly deal with the oversight of the interception procedure, it does contain provisions concerning the general oversight of network operators and service providers operations conferred to the Agency for Electronic Communications (the "Agency") and to the administrative state body for inspection tasks as per Articles 184 and 185. According to Article 189, paragraph 1, subparagraph 6, the Agency monitors the security of an operator's or a service provider's electronic communications network and service and their compliance with the provisions relating to the confidentiality of communications. The Agency under Article 189 paragraph 3 is authorised to order a network operator or service provider to undertake, within a reasonable deadline, measures necessary for adjusting their activities to ensure they are in line with the statutory requirements to keep communications confidential.

Article 180 paragraph 1 obliges network operators and service providers to inform the Agency regarding conditions that network operators and service providers secure technical and organizational capabilities which enable the interception of electronic communications. The Agency, pursuant to Articles 188 and 189, monitors the work of network operators and service providers and is authorised to request a network operator or service provider to correct any irregularity in its technical and organizational settings.

According to Article 183 paragraph 2, control over the measures taken by network operators and service providers for the purpose of ensuring security of retained metadata is performed by the Agency for Personal Data Protection (the "Agency for PDP"). The Agency for PDP is authorised to request information from network operators, service providers and government

agencies performing an interception relating to the collection and protection of personal data of customers. If data is not processed in accordance with the law, the Agency for PDP may order one of the following measures: the rectification of irregularities within a specified period of time; a temporary ban on any data processing carried out contrary to the provisions of the law; and the deletion of personal data collected without proper legal grounds (Article 71 Personal Data Protection Act (Official Gazette of Montenegro nos. 79/2008, 70/2009, & 44/2012, Zakon o zaštitu podataka o ličnosti).

5.3 Police Act (Official Gazette of Montenegro nos. 44/2012, 36/2013 and 1/2015, Zakon o unutrašnjim poslovima) (the "PA")

According to Articles 114, 115 and 119 PA, police activities are generally supervised by a special department of the Ministry of Police for Internal Control, which monitors the legality of police work, especially with regards to the respect and protection of human rights in the performance of police tasks and applying police powers. The Ministry of Police for Internal Control delivers its reports to the Minister of Police and the government at least once a year.

According to Article 112 and 113, police activities are also generally monitored by the Council for Civil Control, a special body comprised of members of the Bar Association, Doctors Association, Lawyers Association, University of Montenegro and nongovernmental human rights organizations, which evaluates police work and provides recommendations for improving their activities to the Minister of Police.

5.4 The Agency for National Security Act (Official Gazette of Montenegro, nos. 28/2005, 86/2009, 20/2011 and 8/2015 Zakon o Agenciji za nacionalnu bezbjednost) (the "ANSA")

Pursuant to Article 40, the work of the ANS is monitored by the Chief Inspector appointed by the Government (the role of which is outlined above - internal control)). Political supervision over the work of the police and the ANS is conferred to Parliament as per Article 110 and 111 PA and Article 43 ANSA.

5.5 Law on Constitutional Court of Montenegro (Official Gazette of Montenegro, no. 12/2015, Zakon o ustavnom sudu Crne Gore)

Network operators and service providers may also file a constitutional appeal against an individual decision of a government agency which violates the constitutional guarantees, when other legal remedies, such as complaints or appeal procedures with the relevant agency or court have been exhausted or are not prescribed or where the right to their judicial protection has been excluded by law (under Article 68 in connection to Articles 48 and 49.

5.6 Constitution of Montenegro (Official Gazette of Montenegro no.1/2007 and 38/2013, Ustav Crne Gore) (the "Constitution")

According to Articles 132 and 133, all measures which would provide for derogation from confidentiality of letters, telephone conversations and other means of communication and protection of personal data, which would be adopted by the Council for the Security and Defence, must be ratified by the Parliament when in a position to convene.

Furthermore, under Article 149, the Constitutional Court of Montenegro, which is authorised to assess constitutionality and legality of laws and other general acts, may find that a measure of derogation introduced during a state of war or a state of emergency is unconstitutional.

6. PUBLICATION OF AGGREGATE DATA ON THE USE OF GOVERNMENT POWERS

There is no law prohibiting the publication of any of the laws mentioned in this report or any description of the powers set out in those laws.

6.1 Electronic Communications Act (Official Gazette of the Republic of Montenegro nos. 40/2013, 56/2013 and 2/2017, Zakon o elektronskim komunikacijama) (the "ECA") and

Under Article 30 paragraph 1 ECA, network operators and service providers must deliver to the Agency for Electronic Communications all available data concerning the development of the electronic communications network or the services provided, with the exception of data relating to intercepted communications and disclosure of metadata. Furthermore, Article 180 paragraph 3 ECA requires network operators and service providers to make a permanent record of all interceptions in collaboration with the government agency that requested the interception. These records must be kept secret.

This indicates that the records of interception activities and requests for provision of metadata by the police and other government agencies (except for the Agency of National Security, see section 6.2 of this report below) may not be published by network operators or service providers. However, there is no law to prevent the publication of aggregate data (i.e. the number) relating to these requests.

6.2 The Agency for National Security Act (Official Gazette of Montenegro, nos. 28/2005, 86/2009, 20/2011 and 8/2015, Zakon o Agenciji za nacionalnu bezbjednost) (the "ANSA")

Article 8 ANSA provides that network operators and service providers must keep secret all details relating to any requests received by the Agency of National Security. Aggregate data relating to these requests, therefore, may not be published.

7. CYBERSECURITY

7.1 Information Security Act ("Official Gazette of the Republic of Montenegro", nos. 14/2010 and 40/16, Zakon o informacionoj bezbjednosti) (the "ISA")

The ISA regulates measures and standards on data information security and is applicable to all state bodies, legal entities

performing a public function, other types of legal entities as well as natural persons who access or process data. Under Articles 1, 3 and 4 however the ISA does not however apply to data for which information security is provided under the rules of data secrecy.

Pursuant to Article 2 ISA, data is defined as any information, message or document created, sent, received, recorded, stored or displayed by electronic, optical or any such similar means, including the use of internet transmission and electronic mail.

Measures of information security are considered to be general rules that provide a basic level of protection of data at a physical, technical and organisational level. Measures of information security under the ISA shall be determined in accordance with type of data, the risks of its safety and the type of protection as per Article 6. Article 6 also prescribes that information security includes measures of physical protection, protection of data and protection of information system. These measures encompass, among other things:

(i) Controlling access to servers and systems through a log-in mechanism available only to authorised persons;

(ii) Implementing mechanisms to prevent the unauthorised export or import of data;

(iii) Implementing forms of protection against computer viruses and other malicious programs;

(iv) The use of backup storage for any collected data;

(v) Implementing the use of crypto-protection of data during its transfer through any information or telecommunication system; and

(vi) Recording any attempts of unauthorised access to any system and recording the related information such as the location from where such access was attempted .

Data operators are obliged to appoint an individual within their organisation to act as their internal Computer Emergency Response Team (the "CERT"). It is the CERT's obligation to notify the CIRT, a directorate within the Ministry of Public Administration, of any breaches of the ISA that may occur. The Ministry of Public Administration (the "MPA") performs the function of a national CERT in relation to any incident suffered under the ISA and works alongside the CIRT pursuant to Article 13 to help affected data operations recover from such incidents.

It is the CIRT who is in charge of the protection of information systems and the prevention of cybersecurity incidents (in particular in regards to the internet as well as from other security risks). Under Article 11, the CIRT is authorised to take:

(i) measures to establish a system of protection;

(ii) measures to prevent cybersecurity breaches; and

(iii) measures to minimise the consequences of any cybersecurity incident that exceeds the capacities of the information system which suffered from it.

Pursuant to Article 14(a), the ISA categorises an information system which is; (i) vital for the performance of a body's/entity's activity (i) is in the public interest; and (iii) which if interrupted or destroyed could jeopardize the lives, health, and security of Montenegro's citizens and the functioning of its State as a "critical information infrastructure".

Whilst the ISA does not further define the term "critical information infrastructure", the former Ministry of Information Society and Telecommunications (which is now part of the Ministry of Public Administration) recognized information technologies and telecommunications as critical information infrastructures in its documents "Strategy for cyber security" and "Methodology for identifying a critical information structure", which are both available on the Ministry's internet site.

Under the ISA, monitoring in regards to compliance with the ISA's provisions is a right conferred upon the Ministry of Public Administration and the members of its special division, the CIRT.

The ISA also obliges legal entities under Article 15 to allow inspectors to access their premises and computer equipment, as well as to present without delay any necessary data and documentation relating to the subject of the inspection. Although the ISA does not stipulate the sanctions that are applied when a legal entity refuses to provide such access, the general rules of the Inspection Control Act ("Official Gazette of Montenegro", nos. 39/2003, 76 /2009, 57/11, 18/14, 11/15 and 52/16, Zakon o inspekcijskom nadzoru) (the "ICA") which is applicable to all inspection controls, provides that the failure to cooperate with an inspector is a misdemeanor punishable with a fine between EUR500 to EUR15,000 for a legal entity and EUR30 to EUR500 for the authorized representative of the legal entity.

As stated above, the CIRT is also authorized to undertake certain measures to eliminate/ reduce the consequences of a cybersecurity incident that overcomes the capacities of the information system which suffered it. The ISA does not specify what the exact function of the CIRT would be in such a situation, though it seems likely that CIRT's would have a certain level of access to the telecommunication system of the information system, deriving out of their power to control and monitor, particularly in cases of recovery from a large scale incident.

As a matter of general rules on data protection and data secrecy, communications related to an incident or any other communications that involves personal data or secret data, have to be conducted in accordance with the rules on data protection and data secrecy. Any failure to do so may constitute a violation of privacy rights.

The ISA does not prescribe a special appeal mechanism for individuals aggrieved by a decision made by the CIRT. However since both the CIRT and the inspectors of the Ministry of Public

Administration are administrative bodies of Montenegro, the rules on appeal processes as provided by the Administrative Procedure Act ("Official Gazette of Montenegro", nos. 56/2014, 20/15 and 40/16, Zakon o upravnom postupku) (the "APA") and the ICA are applicable to decisions made under the ISA provisions. Pursuant to the ICA, an entity that has been subject to an inspection is entitled to;

(i) submit its objections of any minutes recorded of the conducted inspection;

(i) file an appeal against the decision of the inspector to the Ministry of Public Administration; and

(i) initiate administrative court proceedings against the final decision of the Ministry of Public Administration.

All misdemeanour proceedings, which may be initiated against a legal entity that refuses to cooperate with the inspectors during an inspection control, are conducted in accordance with the Misdemeanours Act ("Official Gazette of Montenegro", nos.1/2011, 6/11, 39/11 and 32/14, Zakon o prekrsajima) (the "MA"). The MA provides that an appeal may be filed against a decision of the first instance misdemeanour court to a second instance misdemeanour court.

8. CYBERCRIME

8.1 Criminal Code of Montenegro ("Official Gazette of Montenegro", nos. 70/2003, 13/04, 47/06, 40/2008, 25/10, 32/11, 64/11, 40/13, 56/13, 42/15 and 58/15, Krivični Zakonik Crne Gore) (the "CC")

The CC recognizes the following six criminal offences in the area of cybercrime:

Statutory Reference	Offence	Penalty
Article 349	Damaging Computer Data and Programs Described as, deleting, altering, damaging, concealing or otherwise making unusable a computer data or program without authorisation	Fine or imprisonment up to one year and the seizure of any equipment or devices used in the perpetration of the offence
	If the offence results in damages exceeding EUR 3,000	Imprisonment of three months to three years and the seizure of any equipment or devices used in the perpetration of the offence
	If the offence results in damages exceeding EUR 30,000	Imprisonment of three months to five years
Article 350	Computer Sabotage (Obstruction of computer system) Described as destroying, deleting, altering, damaging, concealing or otherwise making unusable computer data or programs or damaging or destroying computer data or a computer system, with the intent to disrupt the functioning of the computer system	Fine or imprisonment of up to three years and the seizure of any equipment or devices used in perpetration of the offence
	If the above act was committed in relation to data and/or programs which are of relevance to state bodies, public services, enterprises or other entities	Imprisonment of one to eight years and the seizure of any equipment or devices used in the perpetration of the offence
Article 351	Creating and Introducing Computer Viruses Described as making a computer virus with the intent to introduce it into another's computer system	used in the perpetration of the offence
	If the computer virus is successfully introduced into another's computer system and thereby causes damage	Fine or imprisonment of up to two years and the seizure of any equipment or devices used in the perpetration of the offence
Article 352	Computer Fraud Described as entering, altering, deleting, failing to enter correct data or otherwise concealing or falsely representing computer data or interrupting in any way the performance of a computer system and thereby affecting the results of its electronic processing, transfer of data and functionality, with the intent to acquire (for himself or another) unlawful material gain and thus causing material damage to another person or entity	Fine or imprisonment of six months to five years
	If the offence results in the acquisition of material gain exceeding EUR 3,000	Imprisonment of two to ten years
	If the offence results in the acquisition of material gain exceeding EUR 30,000	Imprisonment of two to twelve years
	Where the offence is committed with malicious mischief	Fine or imprisonment of up to two years

Statutory Reference	Offence	Penalty
Article 353	Unauthorised Access to Computer, Computer Network or Electronic Data Processing	Fine or imprisonment up to one year
	Described as accessing a computer system as a whole or part of it without authorisation, or accessing an electronic data process without authorisation	
	If the offence is committed by circumventing protective measures or if it relates to the unauthorised access to a computer system which is of relevance to state bodies, local bodies and enterprises that are authorised to exercise public powers	Fine or imprisonment up to three years
	Also, if the offence involves intercepting computer data that is not publicly available, to, from or within a computer system, including by using electromagnetic emission (regardless of the manner by which such data was transmitted) without authorisation	Fine or imprisonment up to three years
	If an individual uses information obtained in any of the manners above	Fine or imprisonment up to three years
	If by obtaining information in the manner specified directly above resulted in grave consequences for others	Imprisonment of six months to five years
Article 354	Abuse of Devices and Programs Described as producing, selling, obtaining for usage, importing, distributing or in any other way making available: 1) devices and computer programs projected or adjusted primarily for the purpose of committing some of the cybercrimes listed above; or 2) computer codes or any similar data which would allow access to part or whole of a computer system with the intention to use such codes or data for the purpose of committing a crime listed above	Imprisonment of three months to three years
	Owning any item listed above with the intent to use it for committing some of the crimes listed in this section	Fine or imprisonment of one year

The agencies responsible for the prosecution of cybercrimes are the State Prosecutor's office and the police forces within the Ministry of Interior. Judicial decisions are taken by the criminal courts of the Republic of Montenegro.

The Police and the State Prosecutor`s Office are authorized to investigate cybercrimes in accordance with the provisions of the CPC. In principle, both the Police Act ("Official Gazette of Montenegro", nos. 28/2005 and 88/09, Zakon o policiji) (the "PA"), which also regulates the police activities, and the CPC require court approval before undertaking any investigatory measure that could violate someone`s privacy and both contain provisions which guarantees a right to a fair trial.

Moreover, under the CC, the criminal legislation of Montenegro is applicable to foreigners, if they are found on the territory of Montenegro or if extradited to Montenegro, and commit a criminal offence against Montenegro or its citizens outside the territory of Montenegro. A criminal prosecution shall take place if the criminal offence is also punishable by the law of the country where the crime was committed.

Under Articles 137 and 138, the criminal legislation of Montenegro shall also apply to a foreigner who commits a criminal offence abroad against a foreign state or foreign citizen where such offence is punishable by four years' imprisonment or a heavier penalty pursuant to the laws of the country of commission of the crime, if such person is found on the territory of Montenegro and is not extradited to the foreign

state against which the cybercrime was committed.

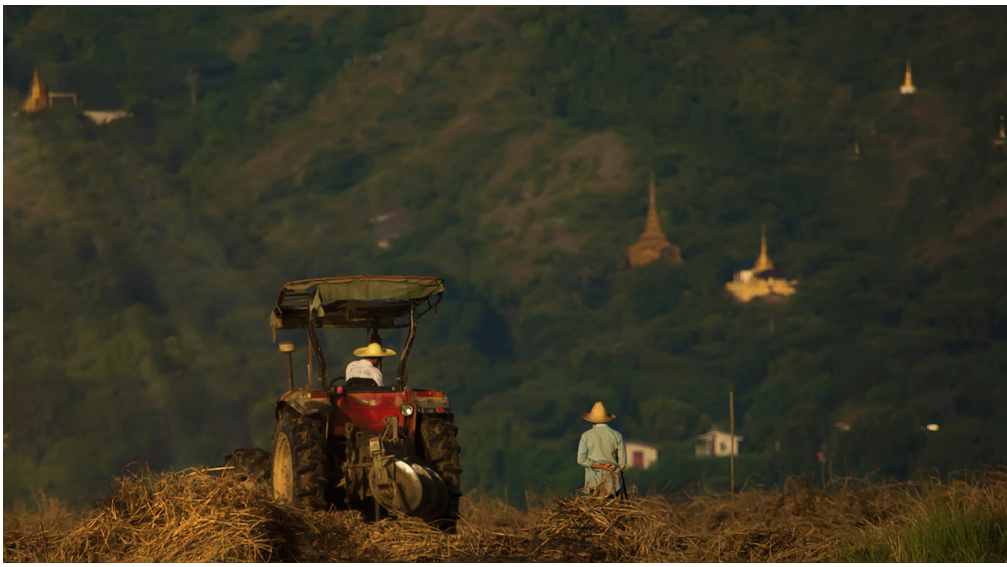
The CPC also provide that an appeal may be filed against a first instance court decision to a second instance court under Article 381.

Law stated as at 20 February 2017.

MYANMAR – 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 Myanmar law.



1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

1.1 Telecommunications Law 2013 (the "2013 Law")

The 2013 Law was drafted to update Myanmar's telecommunications sector and to provide a legal framework for the introduction of foreign private investment in the industry. It repealed the Myanmar Telegraph Act 1895 (the "1895 Act") and the Myanmar Wireless Telegraph Act 1934, although under section 85(b) of the 2013 Law, rules, notifications, orders and directives issued under the older legislation may continue to be applicable insofar as they are not inconsistent with the new law. There are also additional rules and regulations in relation to the 2013 Law, which are at varying stages of coming into force. The first of these are the Licensing Rules, which were introduced by Notification No. 16/2014 on 14 October 2014 (the "Notification").

Under section 75 of the 2013 Law, the government may as necessary direct the relevant organisations to intercept any information or communications that may adversely affect national security or the rule of law and order, so long as the exercise of such powers does not infringe the fundamental rights of the citizens (as set out in the 2008 Constitution of Myanmar).

In general, all service providers wishing to provide network, network facility or application services must be licenced (section 5 of the 2013 Law) and so will be licence holders. Under section 77, the Ministry of Communications and Information Technology (the "MCIT") has wide discretion to direct a licence holder to intercept communications, when it is in the public interest and with the approval of the government. The 2013 Law does not contain a test to determine what constitutes "in the public interest". Section 5(1) of the 1895 Act, however, authorises the President of the Union or an authorised representative, in times of public emergency or in the interests of public safety, to take temporary possession of, block, detain, intercept or disclose any telegraph, which may indicate how "in the public interest" would be interpreted under section 77 of the 2013 Law.

Section 5(2) of the 1895 Act states that if any doubt arises as to the existence of a public emergency, or whether any act done under section 5 (1) was in the interest of the public safety, a certificate signed by a Secretary to the Government is conclusive proof on the point.

In relation to monitoring and enforcement of licences, section 36(a) (ii) of the Notification also refers to a lawful interception request in the context of when a licensee may be exempt from providing certain information to the Telecommunications Department of the MCIT. There is currently no clarification as to what constitutes a lawful interception request.

Section 78 of the 2013 Law provides that a licensee must make necessary preparations to enable a telecommunication service to be utilised for security matters in accordance with the law. This suggests that a telecommunications provider may be required to assist the government in the implementation of interception capabilities on its network.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Telecommunications Law 2013 (the "2013 Law")

Under section 17 of the 2013 Law, a licensee must keep information transmitted or received through its telecommunications service confidential and must not disclose the confidential information of each user to any unauthorised or irrelevant person except for matters allowed by the existing laws (such as those set out in sections 75 to 78, described above).

There is no definition of "irrelevant party" but this may be interpreted to mean any unauthorised third party. Section 36 of the Notification, however, provides that, the Telecommunications Department of the Ministry of Communications and Information Technology (the "Department") may:

(a) establish regular, reasonable reporting requirements on the activities of all or certain categories of Licensees; and

(b) issue a written request to specific licensees for any information, data, document, agreement, operating log, papers or other information required by the Department to discharge its functions under the 2013 Law, provided that such request is reasonable, not unduly burdensome and affords the licensee at least thirty days to provide the requested information unless subject to a lawful interception request.

Under section 36(b) of the Notification, licensees are obliged to comply with this request.

In addition, section 38 of the Notification states that the Department has the authority to inspect the facilities and documents of any licensee, subject to a reasonable notice period prior to inspection and provided that the inspection has a legitimate aim and is proportionate and necessary for the purpose for which inspection is undertaken.

The wording of sections 17 and 69 of the 2013 Law also implies that disclosure may be required in the context of legal proceedings and under a court order. Section 69 of the 2013 Law makes it an offence to disclose any information which is kept under a secured or encrypted system unless in the context of court proceedings relating to telecommunications and when ordered to disclose such information by the court.

Furthermore, section 95 of the Code of Criminal Procedure 1898 (the "Code") states that only a District magistrate, High Court or Court of session may require the delivery to any person they direct of "any document, parcel or thing" that is in the custody of the postal or telegraph authorities in relation to an investigation, inquiry, trial or any other proceeding under the Code.

3. NATIONAL SECURITY AND EMERGENCY POWERS

3.1 Telecommunications Law 2013 (the "2013 Law")

Under section 76, the Ministry of Communications and Information Technology (the "MCIT") or the department or organisation assigned by it may, for defence and security matters of the State or for the public interest, enter into and inspect, supervise and require submission to it of any documents relating to the service activities of the telecommunications service provider. "Service activities" is not defined and there is no detail provided in the law regarding how this section would be implemented. Note, however, that a licensee's permitted activities will also be contained in its individual licence.

4. CENSORSHIP

4.1 Telecommunications Law 2013 (the "2013 Law")

Section 77 of the 2013 Law permits the Ministry of Communications and Information Technology (the "MCIT") to restrict and block certain kinds of communications and to control and use the business of any telecommunications service provider and its telecommunications devices when it is deemed in the public interest and with the approval of the government. The method by which this provision would be enforced is unclear. Under section 22 of the Notification the Telecommunications Department of the MCIT (the "Department") is given authority to direct the Licensee to suspend any services rendered pursuant to a licence or to terminate a licence, either following a breach of the terms and conditions of a licence by the licensee, or failure by the licensee to comply with the duties of a licensee or with any directives or resolutions issued by the MCIT or the Department.

4.2 Electronic Transactions Law 2004 (the "ETL")

The ETL applies to any kind of electronic record and electronic data message used in the context of commercial and non-commercial activities. Section 33 makes it an offence to undertake any act by using electronic transactions technology which is detrimental to the security of the State or prevalence of law and order or community peace and tranquillity or national solidarity or national economy or national culture. This may be interpreted widely.

The method by which this provision may be enforced is unclear.

5. OVERSIGHT OF THE USE OF POWERS

5.1 The Constitution of the Republic of the Union of Myanmar (2008) (the "2008 Constitution")

The 2008 Constitution includes the grant of certain fundamental rights, including of freedom of expression, to each citizen so long as such rights are not exercised in a way that is contrary to laws that are enacted for the security of the state, the prevalence of law and order, community peace and tranquillity or public order or morality. The Constitution also requires the government to protect the privacy and security of correspondence and other communications under the law, subject to its other provisions.

5.2 Telecommunications Law 2013 (the "2013 Law")

As a general comment, one of the overarching objectives of the 2013 Law is to provide legal protection to both telecommunication service providers and to the users of such services.

The Ministry of Communications and Information Technology (the "MCIT") must seek government approval to request an interception under section 75 of the 2013 Law or to block or restrict access to communications under section 77. There is no clarification of what form government approval would take (for example, as an executive order or parliamentary resolution).

However, under section 82, in matters of national emergency, natural disaster or for national defence and security, the MCIT may exempt any government department, organisation or person from obtaining any permission, licence or recommendation required under the law without the prior approval of the government. Such exemptions must, however, be submitted to the government.

5.3 Judicial Oversight

There is no specific judicial oversight process laid out in law. Where disclosure of data is required in the context of legal proceedings, the competent court may control such disclosure.

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

There is no law in Myanmar preventing the publication of aggregate data relating to the use of the powers described above. Furthermore, no law prevents the publication of laws which set out the powers of government agencies or descriptions of those powers.

7. CYBERSECURITY

There is no specific legislation relating to cybersecurity in Myanmar.

8. CYBERCRIME

There is no specific legislation regulating cybercrime in Myanmar.

Law stated as at 15 March 2017

NORWAY – 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 Norway.

1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

1.1 Criminal Procedure Act 1981 ((LOV-1981-05-22-25) Lov om rettergang i straffesaker) (the "CPA")

According to section 216a CPA (which falls under chapter 16a on control of communications generally), the district court may make an order permitting the police to carry out communications surveillance when any person is, with just cause, suspected of attempting or committing an offence that:

- is punishable by imprisonment of 10 years or more; or
- contravenes certain provisions of the General Civil Penal Code (the "Penal Code") (a new version of which entered into force on 1 October 2015) including offences relating to national safety, political espionage, acts of war, and certain drug related crimes, or section 5 of the Export Control of Strategic Goods, Services and Technology Act 1987 (the "ECA"), which is a law dealing with export control and related offences.

"Communications surveillance" may consist of audio surveillance of conversations or other communications conducted to or from specific telephones, computers or other apparatus for electronic communication which the suspect possesses or which it may be assumed he will use. It may also, after an amendment in section 216a CPA in June 2016, consist of transmission of hidden signals to such apparatus for electronic communication as mentioned. This may result in surveillance of other phones than that of the suspect. The preparatory works of the amendments clarify that the police must, after having identified the suspect's phone, cease surveillance of other phones than that of the suspect.

The police may be empowered to conduct an interception themselves, or to order the owner or supplier of a network or service to provide such assistance as is necessary for carrying out the interception. The obligation to assist may apply either to the operator who owns the network used for the communication in question, or to the service provider that provides the communications service in question. The CPA does not identify the specific obligations of network operators or service providers, and the police have wide discretion to determine when assistance is necessary.

In addition, under section 222d CPA, the district court may make an order permitting the police to carry out communication surveillance pursuant to section 216a when there is just cause to suspect that someone will perform an act contrary to certain provisions of the Penal Code, which include offences relating to public safety, murder, robbery or organised crime.

Separately, section 222d CPA also provides that, where the Norwegian Police Security Service (the "PST") has reasonable grounds to believe that a person will commit an act that contravenes section 5 ECA, or certain serious crimes including threats to national security and terrorist financing as set out in the Penal Code, the measures set out in section 216a CPA may be invoked.

The PST is the police security agency of Norway and is responsible for monitoring and securing internal security. Publicly known operational departments include the counter-intelligence, investigation, surveillance and technology units.

Court orders issued to the PST may only be given by a judge with the relevant security clearance and the court order may only be issued by the district court chosen by the head of the Norwegian Supreme Court.

According to section 448 CPA, damages may be awarded to network operators and service providers for any loss caused as a result of requests for assistance by the police, when this is found to be reasonable by the court.

According to section 216d CPA, if there is a serious risk that an investigation will be prejudiced by delay, an interim order from the Norwegian Prosecuting Authority (the "NPA") may take the place of a court order. The NPA, which is part of the Norwegian Council of State (a decision-making body of senior government ministers), is responsible for legal prosecutions in Norway.

When the police issue a decision or request a court order, the decision must be made by the chief of police or deputy chief of police or, in their absence, certain other officials of the prosecuting authority as decided by the chief of police or the authorised deputy with written consent of the senior public prosecutor.

The interim order by the NPA must be submitted to the court for approval as soon as possible, and not later than 24 hours after the interception has begun. If the court considers that illegal interception has taken place, any evidence that has been uncovered will be treated in accordance with the rules on illegally acquired evidence.

According to section 216f CPA, permission for all types of control may not be given for more than four weeks at a time, and must not be longer than strictly necessary. If suspicion of an offence relates to a contravention of chapter 8 or 9 of the Penal Code (offences against the independence and security of the state and offences against the Constitution of Norway and the head of state) such permission may be given for up to eight weeks at a time. However, if an extension is required, the police must obtain a new court order (or a decision must be made by the PST or the NPA as per section 216d CPA).

In the summer of 2016, changes were made to the CPA that enable the police to access non-public information in computer systems, on the same terms as for regular communications surveillance.

According to the new section 216 O, the district court may make an order permitting the police to access non-public information in computer systems when any person is, with just cause, suspected of attempting or committing an offence that:

- is punishable by imprisonment of 10 years or more; or
- contravenes certain provisions of the Penal Code (including offences relating to national safety, political espionage, acts of war, and certain drug related crimes) or section 5 of the ECA.

Permission can only be granted when access is assumed to be of significant importance for solving the case, and that solving the case otherwise would be significantly impeded.

Permission can only apply to the accessing of specific computer systems or user accounts of network-based communication services or storage services controlled by the suspect, or accounts that are assumed to be used by the suspect. The access may include communications, electronically stored data, and other information regarding the use of the computer system or the user account.

In the new section 216 P, certain conditions are laid down regarding who may perform the actions necessary for the access specified in section 216 O, and which technical methods may be used. The access must be performed by qualified personnel under the direction of the police chief, the Police Security Service or other specifically authorised person. The Police may use hacking methods, installation of surveillance software, and carry out break-ins to install technical devices in order to carry out the access.

1.2 Police Act 1995 (Lov om politiet (LOV-1995-08-04-53)) (the "PA")

According to section 17d PA, the district court may – for a period of up to 6 months - make an order permitting the Police Security Service (the "PST") to carry out communication surveillance as set out in section 216a CPA, if there is reason to suspect that an offence under certain sections of the Penal Code will be committed. Such offences include terror offences, threatening national security or an offence against someone in the Royal Family, members of Parliament, the government, the High Court or representatives from similar institutions from other countries.

An order from the chief of the PST or his deputy may take the place of a court order if there is a serious risk of an offence against the Royal Family, members of parliament, the government, the High Court or representatives from similar institutions from other countries and preventative action would be impaired by delay.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Criminal Procedure Act 1981 ((LOV-1981-05-22-25) Lov om rettergang i straffesaker) (the "CPA")

According to section 216b CPA, the court may issue an order permitting the police to carry out other forms of control of communications, which may include requesting metadata for example, when a person is, with just cause, suspected of committing certain offences under the Penal Code that may result in imprisonment of five years or more. Such offences include acts that are a threat to national security, political espionage, terrorism, illegal access to data or programs or certain drug related crimes.

Control of communication includes:

- discontinuation or interruption of the transmission of conversations or other communications conducted to or from specific telephones, computers or other communication devices which the suspect possesses or it may be assumed he will use;
- requiring the owner or provider of the network or service which is being used for the communication to inform the police of which communication devices will, during a specific period of time, be linked or have been linked to the device specified in the first bullet point, and of any other data connected with the communication.

Under section 216c CPA, permission to carry out control of communications may only be given if it will be of substantial

significance to clarify the case and the use of other methods of investigation would be substantially more difficult.

The investigation control measure employed may consist of the police requiring that the owner or provider of the network service informs the police of traffic data and "other data". According to the preparatory works (Ot.prp.nr 64 (1998-99) section 23) of the section, "other data" may be but is not limited to:

- information about the duration of a call;
- the geographical location of a cell phone upon the time of the communication; or
- who was logged on to a computer at the time that the computer was used for communication purposes.

The police and the PST may also, following a court order, carry out control of communications in accordance with section 222d CPA, as described in section 1.1 of this report.

When the obtaining of a court order is likely to lead to a serious risk of delay, the police and the PST may apply for an interim order to be issued by the Prosecuting Authority, using the same procedure as is outlined in section 1.1 of this report in relation to interceptions.

2.2 Electronic Communications Act (Act No. 83 of 04 July 2003) (the "ECA")

Sections 2-7 ECA regulate how long and for what purposes network operators or service providers may retain metadata.

Traffic data must be deleted or rendered anonymous as soon as it is no longer necessary for communications or invoicing purposes, unless otherwise determined by or pursuant to law. Any other processing of traffic data requires the consent of the user.

2.3 Police Act 1995 ((LOV-1995-08-04-53) Lov om politiet) (the "PA")

According to section 17d PA, the district court may issue an order permitting the Norwegian Police Security Service (the "PST") to mandate the disclosure of communications metadata as set out in section 216b CPA and information from computer systems as set out in section 216 O, as well as carrying out other investigatory control measures, if there is reason to suspect that an offence under certain sections of the Penal Code will be committed. Such offences include terror offences, threatening national security or an offence against someone in the Royal Family, members of Parliament, the government, the High Court or representatives from similar institutions from other countries.

3. NATIONAL SECURITY AND EMERGENCY POWERS

In addition to the legislation set out above which makes reference to police powers in national security situations, specifically sections 216a, 216b and 222d of the Criminal Procedure Act 1981 and section 17d of the Police Act, the provisions set out below may provide government agencies with further powers in relation to national security and emergencies.

3.1 General Civil Penal Code (the "Penal Code")

According to section 17 of the Penal Code, no person will be punished for committing an act which would otherwise be an offence if they do so to save someone's person or property from what they believe to be an otherwise unavoidable danger. The circumstances must justify the extent of the act. The police have in some cases used this provision as the legal ground to, for example, jam signals, in instances not covered by the other powers outlined in this report.

In addition, under section 18 of the Penal Code, no person may be punished for an act committed in self-defence. As a result, an otherwise criminal act may be committed in defence against an unlawful attack if the act does not exceed what appeared to be necessary for that purpose. The act in self-defence must be proportionate to the danger of the attack, the guilt of the assailant or the legal right that is threatened by the attack.

Provided that the conditions in section 18 are fulfilled the provision may, for example, be used to block other frequencies than those that are part of a public communication network, as provided by section 6-2a ECA and section 216b CPA, for example, to trigger explosives.

3.2 Electronic Communications Act (Act No. 83 of 04 July 2003) (the "ECA")

According to the section 6-2a ECA, the police may use frequencies allocated to others through the use of "mobile regulated zones", subject to certain limitations.

Section 1-5, number 19 ECA defines a "mobile regulated zone" as a limited geographical area where communication in an electronic public communication network for public use is influenced or impaired by use of legal identification catching or jamming. Number 20 of the same section describes "identification catching" as the manipulation of networks used for public mobile communication for the purpose of uncovering the electronic identity of terminal equipment using the network.

The National Security Authority (the "NSA") may also, in exceptional cases and for a short period of time, use frequencies allocated to others without permission from the Norwegian Communication Authority (the "NCA") when this is a necessary measure for proper securing of conference rooms, cf. Section 16 of the Norwegian Security Act.

Both the police and the NSA must also notify the NCA without undue delay after the measure has been established if frequencies allocated to others are used.

The NCA decides, in consultation with the police or the NSA, if a network operator or service provider should be informed. If it is decided that a network operator or service provider should not be notified, this decision must be recorded and explained in writing. According to the preparatory works of the ECA

(Prop.69 L (2012-2013)) Endringer i ekomloven), the NSA and the police must balance the police's need for secrecy against the consequences for the network operator or service provider.

As a result of the use of mobile regulated zones, network operators or service providers may appear to experience irregularities in their systems. In order to avoid costly and unnecessary corrective actions, the police or the NSA will decide, on a case by case basis, whether the network operator or service provider should be informed that the irregularities may be due to the use of a mobile regulated zone. The decision is not subject to disclosure or appeal.

3.3 Ministry of Transport and Communication, public consultation regarding proposed changes to the Police Act and the Electronic Communications Act (Høring – forslag til endringer i politiloven og ekomloven – mobilregulerte soner mv.) (the "Consultation")

The Consultation proposes to amend section 6-1 ECA and section 7b PA. These amendments will give the police permission to establish mobile regulated zones in a greater number of scenarios than the law currently provides for, for example, to prevent serious disruptions of public peace and order or to prevent criminal actions with prison sentences of more than three years.

In addition, mobile regulated zones may be used to identify and block signals in networks other than just the public communication network, for instance, to block explosives that may be triggered by alarm systems or garage openers.

Network operators or service providers need not be notified if this is necessary to implement measures under the new section 7b. The decision not to notify network operators or service providers depends on a cooperative decision made by the police and the NCA, with the final word belonging to the police.

Furthermore, in certain situations the police will not be obliged to notify the NCA. This will only be applicable in a few special situations where there is a serious reason that makes it necessary to keep the police operation secret. If the new rules are implemented, the police will not have to obtain a court order to establish the mobile regulated zone. The decision may be made by the chief of police or the deputy chief of police.

The deadline for responding to the public consultation was 23 January 2015. As of 21 February 2017, no further developments had taken place.

4. CENSORSHIP

4.1 Constitution of the Kingdom of Norway (the "Constitution")

Censorship is prohibited under Article 100 of the Constitution. Certain laws do, however, provide government agencies with powers to block communications in specific circumstances, as set out below.

4.2 Criminal Procedure Act 1981 (Lov om rettergang i straffesaker (LOV-1981-05-22-25) (the "CPA"))

As set out in section 2.1 of this report, according to section 216b CPA, the district court may make an order permitting the police to carry out other forms of controls of communications when a person is, with just cause, suspected of committing certain criminal acts. The control may be exercised by discontinuing or interrupting the transmission of conversations or other communication conducted to or from specific telephones, computers or other communication devices that a suspect possesses or which it may be assumed that he will use.

The communication device must be identified, for instance by a telephone number or IP-address, in the court order. If communications to and from a specific IP addresses are to be blocked, the IP address, must be specific to that computer. If, for example, the computer is given a new IP address each time it connects to the Internet, the IP address is not suitable to identify that computer and the network operator or service provider cannot be ordered to block access to that IP address.

The police must be able to demonstrate a possibility that the device will be used based on objective criteria.

5. OVERSIGHT OF THE USE OF POWERS

5.1 The Communications Control Committee (Kontrollutvalget for kommunikasjonskontroll) (the "Committee")

In relation to the various police powers mentioned above, the Committee must verify that the police's use of their control of communication powers occurs within the confines of the law and that the use of these powers is minimised as much as possible, for example, by ensuring they are only used when necessary for an investigation.

The legal basis for the Committee's authority comes from chapter 2 of the Statute Regarding Communication Control 2000 (the "Communication Statute") and section 216h of the Criminal Procedure Act 1981 (the "CPA").

The Committee evaluates reports from the chief of police to the Office of the Public Prosecutor. It also evaluates any complaints from persons or organisations that claim to have been subject to illegal forms of control of communication. The Committee may also, at its own initiative, look into any case or matter in relation to the police's and the prosecuting authority's use of control of communication. The Committee does not evaluate on-going cases at the request of the prosecuting authority.

According to section 13 of the Communication Statute, the Committee must consist of three members and one or more deputies and the leader of the Committee must fulfil the requirements of a High Court judge.

Under section 17 of the Communication Statute, if the Committee finds reason to criticize the police or the NPA, the matter must be reported to the Attorney General and the Ministry of Justice.

5.2 The Norwegian Parliamentary Intelligence Oversight Committee (EOS-komiteen) (the "EOS Committee")

The EOS Committee is responsible for external and independent control of the Norwegian secret services (including the Police Security Service) (the "EOS Services"). The EOS Committee's primary task is to make sure that the EOS services keep their activities within the legislative framework applicable to them and must further ensure that no individual is subjected to unjust treatment. They must also ensure that the EOS Services do not make use of more intrusive methods than necessary under the circumstances.

The EOS Committee has seven members, including the Chair and Deputy Chair. The activities of the EOS Committee are subject to the Act relating to the Oversight of Intelligence, Surveillance, and Security Services of 3 February 1995 no. 7 (the "Oversight Act"). Provisions in the Oversight Act are supplemented by the Directive relating to the Oversight of Intelligence, Surveillance and Security Services of 30 May 1995 no. 4295, as determined by the Norwegian Parliament.

The EOS Committee submits a report on its activities to the Norwegian Parliament every year. Under Section 8 of the Oversight Act these reports cannot be classified. Prior to submitting the report to the Norwegian Parliament, the EOS Committee verifies that the requirements for releasing the document without classification have been met, by forwarding it to the EOS services involved. Statements in relation to complaints must also be unclassified. Information regarding whether any person has been subjected to surveillance activities will be classified, unless otherwise decided. Statements to administration will be classified according to their content.

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

Restrictions on network operators and service providers

The government does not have the legal authority to prevent a network operator or service provider from publishing aggregate data in relation to the volume of requests from the government it receives relating to the powers described in this report.

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

7.1 Act relating to the Protection of Personal Data (Personopplysningsloven) (the "PPD") and the Regulation on Protection of Personal Data (Personopplysningsforskriften) (the "RPPD")

The PPD and RPPD are both based on the EU Directive 95/46EC and will be replaced in May 2018 with the implementation of the General Data Protection Regulation (the "GDPR"). Also note that the Act on Human Rights (Menneskerettsloven) incorporates the European Convention on Human Rights (the "ECHR") into Norwegian law, particularly where Article 8 (the right to respect for private and family life) becomes highly relevant for the purposes of data protection legislation.

Security breaches and the use of information systems in breach of established routines shall be treated as deviations of cybersecurity legislation as per Section 2-6 RPPD. If a deviation results in the unauthorised disclosure of personal data that is subject to the laws of confidentiality, the entity affected by the deviation is under an obligation to notify the DPI as per the third paragraph of Section 2-6 RPPD. An example of where this obligation would be triggered would be where there has been a hacking of an entity's customer database, which has consequently exposed the personal information of the entity's customers and put them at risk of identity theft.

Individuals must be notified of any situation that has caused their personal data to be unlawfully disclosed, according to case law from the Privacy Appeals Board (Personvernnemnda). How this notification is given must be decided taking into account the severity of the breach, the sensitivity of the data and the potential consequences for the individuals affected.

The Data Protection Inspectorate (Datatilsynet) (the "DPI") is responsible for monitoring and supervising compliance with the both the PPD and RPPD. To do so, the DPI has the ability to:

(a) under Section 44 PPD, demand the disclosure of information without paying regard to the duty of confidentially. The DPI may additionally demand access to sites where personal data registers are placed, sites where the processing of personal data takes place and access to the tools used for such data processing; and

(b) under Section 46.4 PPD, order that the processing of data in violation of the PPD or RPPD shall be stopped, or set specific conditions before the processing of the personal data can continue.

Decisions made by the DPI may be appealed to the Privacy Appeals Board which acts as an independent appeals body. Decisions of the DPI may also be brought before the regular courts of Norway for the purposes of appeal.

The penalties for non-compliance with the PPD include:

- fines issued by the Data Protection Authority of up to NOK 925 760;
- coercive fines issued in accordance with Section 7-2d of the Act on Enforcement; and
- criminal prosecution by the Norwegian Prosecution Authority, which may result in the imposition of fines or a maximum 1 year imprisonment.

7.2 Act relating to Protective Security Services ("Sikkerhetsloven") (the "PSS")

The PSS applies to public entities and to any legal person who

is a supplier of goods or services to an administrative agency in connection with a classified procurement.

Section 29 PSS lays down several conditions that are applicable to public entities proposing to procure critical infrastructure, which is defined under the Act as "facilities or systems necessary to maintain basic needs and functions of society". Specifically, Section 29 sets down obligations on such public entities to carry out risk assessments in relation to their cybersecurity systems and to notify the superior Ministry if a procurement may result in the establishment of an activity that poses a threat to security. In these latter types of cases, the King in Council may decide that the procurement shall be stopped, or that the risk shall be mitigated by outlining certain conditions for the procurement to adhere to before it may proceed.

The main responsibility for monitoring and supervising compliance with the PSS is held by the National Security Authority ("Nasjonal sikkerhetsmyndighet") (the "NSM"). The NSM is to be provided with unhampered access to any area where there is sensitive information or a sensitive object held, insofar as necessary for implementing their supervisory functions.

Pursuant to the first paragraph of Section 5 PSS, an agency regulated by the PSS must notify the superior Ministry or the Ministry of Defence if they have information concerning a planned or on-going activity that may cause a "non-insignificant" risk for any activity that poses a threat to security.

It is the King in Council who may make the necessary decisions to stop a planned or on-going harmful activity that is threatening security ("sikkerhetstruende virksomhet") from continuing. Examples of such activity include the preparation, attempt or execution of espionage, sabotage or terrorist acts. Such decisions are made in line with the second paragraph of Section 5A PSS and are enforceable in accordance with Chapter 13 of the Act on Enforcement ("Tvangsfullbydelsesloven"). This section was described as a "security vent" when initially being drafted, meant only for use in extraordinary circumstances. It is therefore meant for use in only rare and serious cases due to the fact that it provides the King in Council with wide powers. The means chosen to deal with the planned or on-going harmful activity threatening security shall not be more burdensome than what is necessary taking into account the risks at hand.

There is no appeal mechanism in place under the PSS for an individual or entity aggrieved by a decision made by the King in Council. If an individual or entity wishes to appeal such a decision, they must file a case with the Norwegian courts.

Failure to comply with the PSS may result in criminal prosecution resulting in an imprisonment sentence of up to six months under Section 31, unless the acts are punishable under stricter legislation (typically the General Civil Penal Code).

7.3 Act relating to Electronic Communications (Act No. 83 of 04 July 2003) (the "ECA")

The ECA applies to providers of electronic communication networks or services. The Act is monitored and supervised by the National Communications Authority (Nasjonal kommunikasjonsmyndighet) (the "NCA"). Providers of electronic communication networks or services are under a duty pursuant to Section 10-3 to disclose information to the NCA that is necessary for the implementation of the ECA or decisions made in accordance with the ECA.

Where there is particular risk of a cybersecurity breach and if a cybersecurity breach could damage or destroy a subscriber's or user's retained data or infringe their data protection, the provider of the electronic communication networks or services shall immediately notify the subscriber or user of this risk. Notification to the subscriber or user is not necessary under Section 2-7 ECA where the provider can show the NCA that satisfactory technical protective measures have been carried out for the data affected by the security breach.

In ensuring compliance with the ECA, the NCA may;

(a) order providers of electronic communication networks or services to implement restrictions on the use of their networks and services in the interest of national security or other important societal considerations. Pursuant to Section 2-5, providers shall also, without an order from NCA, implement necessary restrictions on the use of their networks or services in emergency situations that involve serious threats to life or health, safety or public order or danger of sabotage against networks or services;

(b) issue regulations on the duty of confidentiality and make case-by-case decisions, pursuant to the fifth paragraph of Section 2-9 and the second paragraph of Section 2-10, to ensure that providers implement measures that provide proper secrecy and preparedness to any data they hold. Note that providers of electronic communication networks and services have an active duty under Section 2-9 in any event to maintain secrecy/confidentiality regarding the content of their electronic communications, and any third party use of their electronic communications). Providers also have a duty to ensure the preparedness and availability of their electronic communications; and

(c) make spot checks, measurements and any other checks without prior notice to the provider under Section 10-1.

The powers of the NCA do not have any significant adverse effects on an individual's rights to privacy and a fair trial.

Decisions made by the NCA can be appealed under Section 11-6 to the Ministry of Transport and Communications.

According to Section 12-4, a breach of the ECA may result in a criminal prosecution resulting in liability to a fine or an imprisonment sentence of up to 3 years.

8. CYBERCRIME

8.1 The General Civil Penal Code ("Penal Code")

On October 1 2015, Norway's new Penal Code entered into force. The new code has several provisions relevant to cybercrime, with Chapter 21 on the protection of information and communication containing more specific provisions directly aimed at the prevention and prosecution of such crimes.

The main cybercrimes covered by the Penal Code are as follows;

Statutory Reference	Offence	Penalty
Section 201 Penal Code (This section implements Article 6 of the European Council Convention of 23.11.2001 on Cybercrime)	Creating, acquiring, possessing or making available: (a) passwords or other information that may give access to information systems or computer systems; or (a) software or anything else particularly designed for committing crimes directed at information systems or computer systems with the intention of committing a criminal act.	Fines or up to one year imprisonment.
Section 204 Penal Code	Breaking a protection or by any other means gaining unauthorised access to a computer system. (Note that this provision relates to the unauthorised access itself. Further unauthorised use of the system, such as searching for, changing or deleting data, will be covered by other provisions, such as the provisions in Chapter 28 on vandalism and damage to property).	Fines or up to two years imprisonment.
Section 205 Penal Code	Violating the right to private communication, by: (a) the use of a technical device to secretly intercept or record conversations between others, or negotiations in closed meetings to which the person does not participate himself, or which he has accessed without authorisation; (b) breaking protection or in another unjustified manner accessing information transferred by electronic or other technical means; (c) opening letters or closed written messages addressed to others, or by other means gaining access to such messages; or (d) hindering or delaying the reception of a message by hiding, changing, destroying or withholding the message.	Fines or imprisonment of up to 2 years.
Section 54 of the Act relating to Intellectual Property Rights (the "IPR")	Violation of copyright.	Fines or imprisonment of up to 3 years. (Note that violations of copyright are generally investigated and prosecuted by the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim).

In addition to the above, Chapter 21 IPR contains provisions for the prevention of crimes such as identity theft, unauthorised access to TV-signals, violation of trade secrets and violation of duty of confidentiality.

Compliance with the Penal Code is regulated by the Norwegian police and the Norwegian Prosecution Authority on the basis of the rules set down in the Act relating to Criminal Procedure.

The territorial reach of the Penal Code is set down in Sections 4 to 8. Section 7 is the important provision for hacking activities carried out by non-nationals abroad. In accordance with Section 7, criminal acts that are carried out abroad can be considered to have been carried out in Norway, if the act has had effect or was meant to have effect in Norway. Accordingly, hacking activities carried out by non-nationals and directed at Norwegian citizens or entities in Norway may be prosecuted in Norway in accordance with Norwegian law.

Decisions and judgements made in accordance with the Penal Code can be appealed pursuant to Part 6 of the Criminal Procedure Act to the relevant court of appeal.

8.2 Future legislation: Digital Border Defence (Digitalt grenseforsvar) (the "DBD")

In September 2016, a public committee appointed by the Ministry of Defence delivered their report which made recommendations on the establishment of a Digital Border Defence. This proposed system, which will be administered by the Norwegian armed forces' secret services, will enable the secret services to intercept all data flow through cables to and from Norway.

Even though access to information gathered through the Digital Border Defence will be supervised by a judicial process in the courts, the initiative is highly controversial and has been subject to extensive criticism by, among others, the Data Protection Inspectorate. The report has been out on public consultation, and is currently under evaluation by the Ministry of Defence for the potential proposal of new legislation. The initiative is likely to be the subject of extensive debate before any legislation is adopted by Parliament (Stortinget).

Law stated as at 21 February 2017.

PAKISTAN – 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 Pakistani law.

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

1.1 Pakistan Telecommunication (Re-Organisation) Act 1996 ("PTRA")

Under section 54 of PTRA, the federal government of Pakistan may authorise any person to intercept calls or messages, or to trace calls made through any telecommunications system for national security reasons or for the investigation of any crime. The Pakistan Telecommunication Authority ("PTA") carries out the interceptions as explained in paragraph 1.2 below. Section 54 is generally regarded as providing a very wide scope for the lawful interception of communications under Pakistani law.

Under section 8 of the PTRA the Federal Government may issue legally binding policy directives to the PTA in relation in relation to certain telecommunications matters, including the requirements of national security. Section 8 also grants the Cabinet, or any committee authorised to do so by it, a broadly expressed power to issue policy directives to the PTA, so long as they are not inconsistent with the provisions of the PTRA. The section 8 powers appear to be used to issue directives relating to lawful interception to operators of telecommunications networks and providers of telecommunications services licensed to operate in Pakistan ("Network Operators").

To give one publicly available example, the PTA made a directive on 21 July 2011 prohibiting the use of all encryption mechanisms which conceal communication to the extent that Network Operators cannot monitor it under the Monitoring and Reconciliation of Telephony Traffic Regulations 2010, the scope of which is set out below.

1.2 Monitoring and Reconciliation of Telephony Traffic Regulations 2010 ("MRTT Regulations")

Regulation 4 of the MRTT Regulations sets out mandatory obligations on certain categories of Network Operator to establish systems that enable, among other things, the monitoring of all telecommunication traffic (voice and data) passing through their networks. Regulation 4 makes provision for the Network Operators to comply with these obligations by entering into mutual arrangements with other Network Operators to deploy a collective monitoring system, subject to the approval of the PTA.

Regulation 4(6) sets out more specific requirements for these systems, including that they enable the monitoring, measuring, controlling and recording of traffic in real-time, that they maintain a complete record of all communication signals (including for, but not limited to, billing purposes) and that they maintain a complete list of all Pakistani customers and their details. The monitoring systems must be compatible in order that all this information can be provided to the PTA as required.

Regulation 4(7) states that no person, except the PTA, is allowed to monitor any traffic directly or indirectly on their own or another network without the written permission of the PTA.

Under Regulation 5(8), those Network Operators licensed to operate telecommunications infrastructure, to provide long distance and international telephone services, or to operate local loop (fixed and wireless) and cellular mobile services must provide authorised representatives of the PTA access to obtain information, directly through the system, that relates to any traffic routed through their network, as and when required by the PTA.

The MRTT Regulations gives the PTA legal authority to have real-time access to many Network Operators' networks and services. They do not contain any provisions requiring the PTA to inform the Network Operators that such access has taken place.

1.3 Federal Investigation Agency Act 1974 ("FIAA")

Under section 5 of FIAA, the Federal Investigation Agency ("FIA") has the right to carry out investigations for the purposes of detecting or preventing any crimes under a variety of different laws, including but not limited to those under the Official Secrets Act 1923, the Drugs Act 1976, the Anti-Terrorism Act 1997 (to the extent that the federal government of Pakistan has granted the FIA the authority) and the PTRA. These investigations may require the interception of private communications.

1.4 Investigation for Fair Trial Act 2013 ("IFTA")

Under sections 4-8 of IFTA, certain government agencies may apply to the High Court for a secret warrant permitting the interception or surveillance of any form of digital communication for the purpose of collecting evidence, including the seizure of computing equipment, where the subject of the warrant is suspected of involvement with terrorism-related offences. The agencies in question include the Inter-Services Intelligence, the Intelligence Services of the three branches of the Armed Forces of Pakistan, the Intelligence Bureau and the Police (together the "Intelligence Services").

The scope of IFTA, therefore, is limited to the investigation of terrorism-related offences identified in various laws specified in IFTA, for example the Anti-Terrorism Act 1997 ("Scheduled Offences"). As such the powers of interception that IFTA grants are more limited than those under the PTRA. However, where an intelligence agency wishes to admit evidence to court in the course of a trial on terrorism-related activities related to the Scheduled Offences, it must have obtained a warrant from the court under IFTA.

Before obtaining the warrant, section 16 of IFTA provides that the Intelligence Service must obtain authorisation from the Minister of the Interior. The procedure for obtaining this authorisation is set out in more detail in paragraph 5.2 below. The court warrant is limited in scope to the activities authorised by the Minister of the Interior. The Minister may authorise the use of any technology for the carrying out of interceptions, and may direct Network Operators to implement any technology required to comply with the warrant.

1.5 Prevention of Electronic Crimes Act 2016 ("PECA")

Real-time collection and recording of information

Under section 39 of PECA a duly authorized officer may apply to the Court of competent jurisdiction to collect real time information as well as to collect or record such information in real-time in coordination with the investigation agency. The authorized officer means an officer of the FIA who is duly authorized on behalf of FIA to perform any function of the Investigation Agency, i.e. FIA, under PECA.

The Court may pass orders authorizing the FIA to collect real time information as well as to collect or record such information in real-time in respect of information held by or passing through a service provider provided that the Court has reasonable grounds to believe that the content of any information is reasonably required for the purposes of a specific criminal investigation and the duly authorized officer can:

(a) explain why it is believed that the data sought will be available to the person in control of an information system;

(b) identify and explain with specificity the type of information likely to be found on such information system;

(c) identify and explain with specificity the identified offence made out under PECA in respect of which the warrant is sought;

(d) if authority to seek real-time collection or recording on more than one occasion is needed, explain why and how many further disclosures are needed to achieve the purpose for which the warrant is to be issued;

(e) specify what measures shall be taken to prepare and ensure that the real-time collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information of any person not part of the investigation;

(f) explain why the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and

(g) explain why, to achieve the purpose for which the warrant is being applied, real time collection or recording by the person in control of the information system is necessary.

(h) Real-time collection or recording shall not be ordered for a period beyond what is absolutely necessary and in any event for not more than seven days. Further, notwithstanding anything contained in any law to the contrary, the information collected shall be admissible as evidence in Court. Additionally, the period of real-time collection or recording may be extended beyond seven days if, on an application, the Court authorizes an extension for a further specified period. Finally the Court may also require the designated agency to keep confidential the fact of the execution of any power provided for under section 39 and any information relating to it.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Monitoring and Reconciliation of Telephony Traffic Regulations 2010 (the "MRTT Regulations"), the Federal Investigation Agency Act 1974 ("FIAA") and the Investigation for Fair Trial Act 2013 ("IFTA")

The provisions of the MRTT Regulations, FIAA and IFTA as set out in paragraphs 1.2 to 1.4 above also apply to the collection and disclosure of communications data.

Under the MRTT Regulations, operators of telecommunications networks and providers of telecommunications services licensed to operate in Pakistan ("Network Operators")

must configure their systems to enable the Pakistan Telecommunications Authority ("PTA") to carry out certain activities including but not limited to monitoring, controlling, measuring and recording all traffic over the network in real-time, as set out in paragraph 1.2 above.

2.2 Code of Criminal Procedure 1898, as amended ("CCrP")

Under section 94 of CCrP, a court or a police officer in charge of a police station may order the production of 'any document or other thing' if they consider that it is necessary or desirable for the purposes of the investigation of a crime (subject to limited exceptions). This means that legal persons in Pakistan can be required to produce a wide range of information, which may include data relating to private communications, to the court or to an officer in charge of a police station, under section 94. Refusal to produce the required information can be punished by a fine or a prison sentence, or both.

2.3 Prevention of Electronic Crimes Act 2016 ("PECA")

Under section 32 of PECA a service provider shall, within its existing or required technical capability, retain its specified traffic data for a minimum period of one year or such period as the Authority may notify from time to time and subject to the production of a warrant issued by the Court provide that data to the investigation agency or the authorized officer whenever so required.

Violation of this section by a telecommunications service provider or network operator shall be deemed to be a violation of the terms and conditions of its licence and shall be treated as a such under the PTRA.

Note that PECA also contains a number of general powers relating to the acquisition, preservation, search or seizure and inspection of data held on information systems as may be reasonably required for the purposes of a criminal investigation or criminal proceedings. These powers are also subject to the authority of the Court.

3. NATIONAL SECURITY/EMERGENCY POWERS

3.1 Pakistan Telecommunication (Re-Organisation) Act 1996 ("PTRA")

As stated in paragraph 1.1 above, section 54 of PTRA grants the federal government of Pakistan the power to authorise any person to intercept any form of private communications on the ground of national security, and so the procedure for interception as set out in that Act applies in cases of national security.

Section 54 (3) of PTRA also provides that, in the event that the President of Pakistan declares a national state of emergency, the federal government has the power to modify all licences granted to operators of telecommunications networks and providers of telecommunications services licensed to operate in Pakistan ("Network Operators"), and the federal government can order the immediate suspension of Network Operators' networks or any of their individual services. The government has used section 54 to suspend and shut down services, as well as intercept communications, during periods of national emergency.

Under section 54(2) of PTRA, in a time of war or civil unrest, the federal government of Pakistan has priority use of any telecommunications networks.

Under section 8(2)(c) of the PTRA, the federal government may make specific directives to the Pakistan Telecommunication Authority ("PTA") in relation to the requirements of national security on telecommunications networks.

3.2 Investigation for Fair Trial Act 2013 ("IFTA")

Sections 4-8 of the IFTA, as described in paragraph 1.4 above, also allows interceptions of communications on grounds of national security since it gives powers for preventing terrorism activities that may fall under the Scheduled Offences.

3.3 Prevention of Electronic Crimes Act 2016 ("PECA")

Under section 49 of PECA the Federal Government may constitute one or more computer emergency response teams to respond to any threat against or attack on any critical infrastructure information systems or critical infrastructure data, or widespread attack on information systems in Pakistan. A computer emergency response team shall respond to a threat or attack without causing any undue hindrance or inconvenience to the use and access of the information system or data as may be prescribed.

4. CENSORSHIP RELATED POWERS

Power to shut down networks or service categories

4.1 Pakistan Telecommunication (Re-Organisation) Act 1996 ("PTRA") and Pakistan Telecommunication Rules 2000 ("PTR")

Under section 21(4)(f) of the PTRA, all licences granted by the Pakistan Telecommunication Authority ("PTA") to operators of telecommunications networks and providers of telecommunications services ("Network Operators") may, among other things, contain a provision requiring a Network Operator to terminate a telecommunications service provided to a user who has misused the service and continues to misuse it having been informed of such misuse by the Network Operator.

Under section 9 of the PTR, the PTA may monitor compliance by Network Operators with the terms of their licences and their obligations under the PTRA. Once a written notice has been sent to a Network Operator by the PTA alleging any breach of the terms of its licence, the Network Operator has 30 days to demonstrate that the issue has been resolved. If the alleged contravention remains unresolved the PTA may issue an enforcement order, and if the contravention still persists 30 days after the serving of the order, then the PTA may order the termination of the Network Operator's licence.

As set out in paragraph 3.1 above, following the declaration of

a state of emergency by the President of Pakistan, the federal government can suspend any or all licences of Network Operators. Also, as set out in paragraph 3.1 above, the federal government has used s. 54(2) of PTRA to shut down or suspend telecommunications networks or certain services in a time of war or of civil unrest. At present, this latter power is exercised frequently by the federal government to shut down text messaging and other cellular network services in Pakistan.

Blocking of web pages and IP addresses

Under section 31(d) of PTRA, the dissemination of electronic or digital information which is considered false, indecent or obscene is a criminal offence. However, 'false', 'indecent' and 'obscene' are not specifically defined in PTRA.

4.2 Inter-Ministerial Committee for the Evaluation of Websites ("IMCEW") and Pakistani Penal Code 1860, as amended (the "Pakistani Penal Code")

In 2006 the Prime Minister of Pakistan created the IMCEW with a mandate to restrict offensive online content. It consists of representatives from government ministries including the Ministry of the Interior, the PTA, the Cabinet and the security services. Where IMCEW decides that a website or IP address should be blocked, the Pakistani Ministry of Information Technology directs the PTA to perform the blocking.

The term 'offensive' is not specifically defined in Pakistani law in relation to online content. In line with the provisions of the Pakistani Penal Code relating to offensive conduct, it seems likely that online content which is deemed to be offensive will include content that offends a wide range of religious beliefs in Pakistan. This includes (but is not limited to), content that injures or defiles places of worship, content including words that deliberately attempt to wound religious feelings or derogatory remarks in respect of holy people, insults to religion that are intended to incite outrage, and misuse of descriptions or titles of religious groups.

4.3 Prevention of Electronic Crimes Act 2016 ("PECA")

Under section 37 of PECA the Authority shall have the power to remove or block or issue directions for removal or blocking of access to any information through any information system if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under PECA.

4.4 Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communications Regulations 2009, as amended ("SUFOC Regulations")

The SUFOC Regulations provide that Network Operators must have procedures in place, approved by the PTA, to minimise spam emails and any unsolicited, fraudulent and obnoxious communications.

Under regulation 5 of the SUFOC Regulations, all Network Operators must maintain blacklists of those who have made fraudulent communications over their network. Once a customer has been involved in sending a fraudulent communication on more than one occasion, they will be banned from subscribing for any cellular mobile services.

Network Operators must also maintain blacklists of telemarketers who have violated their licence to conduct telemarketing activities under regulation 6 of the SUFOC Regulations. Customers on this blacklist will not be permitted to obtain another licence to conduct telemarketing.

Regulation 10 and Annex C of the SUFOC Regulations also provide that Network Operators must make blacklists and greylists of customers who have made obnoxious communications. These are messages transmitted over the network with the intention to cause harassment or distress. Customers on greylists will have their services restricted, while those on a blacklist will be limited to only making emergency calls on their network.

Unauthorized issuance of SIM cards etc.

4.5 Prevention of Electronic Crimes Act 2016 ("PECA")

Under section 17 of PECA states that whoever sells or otherwise provides subscriber identity module (SIM) card, re-usable identification module (R-IUM) or universal integrated circuit card (UICC) or other portable module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless phones or other digital devices such as tablets without obtaining and verification of the subscriber's identity in the mode and manner for the time being approved by the Authority shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

5. OVERSIGHT OF THE USE OF THESE POWERS

5.1 Pakistan Telecommunication (Re-Organisation) Act 1996 ("PTRA")

Lawful interceptions of private communications under PTRA are not subject to any additional oversight procedures, and nor is there any appeals process for particular individuals who believe that their information has been unfairly collected.

5.2 Investigation for Fair Trial Act 2013 ("IFTA")

To obtain a warrant under IFTA, sections 6-7 provide that the Inter-Services Intelligence, the Intelligence Services of the three branches of the Armed Forces of Pakistan, the Intelligence Bureau or the Police (an "Intelligence Service") must make a report to the Federal Minister of the Interior. The minister will then permit the Intelligence Service in question to go before a judge of the High Court of Pakistan if he deems there to be a reasonable threat that a terrorism offence may be committed, and that an interception of communications would provide evidence of this.

The hearing before a judge must take place in chambers and the authorised officer must personally present the application. Under section 10(b) of IFTA, a warrant will only be granted if the

judge deems there to be a reasonable threat of a terrorist act about which an interception of communications will provide evidence.

The warrant will allow interception activities to take place for up to 60 days, which is renewable on a further application to the court. The Intelligence Service that has received a warrant then approaches the relevant Network Operator directly and they are legally obliged to implement the interception or maintain the surveillance activity (as applicable). The Network Operator has a general duty of co-operation with the relevant Intelligence Service and must ensure confidentiality in relation to the assistance that it gives in relation to the warrant. Network Operators enjoy immunity from prosecution for their activities under IFTA.

The court warrant may authorise any form of surveillance or interception to take place. Therefore, it is possible that the Intelligence Services would be able to access private communications and related data without notification to the Network Operator. Furthermore, as the court hearing takes place in secret, there is no opportunity for the subject of the interception or surveillance to appeal until the evidence is brought before a court in relation to any crime committed.

5.3 Constitution of Pakistan and the Freedom of Information Ordinance 2002 ("FIO")

Article 19-A of the Constitution of Pakistan states that all citizens must have the right to access information in all matters of public importance, subject to reasonable restrictions imposed by the law.

Under the FIO, no citizen will be denied access to records held by public bodies unless disclosure of that information would, among other things, harm relations between Pakistan and other countries, cause an offence to be committed, prejudice an investigation, invade the privacy of any individual other than the requestor, or cause significant damage to the financial interests of any party.

Under section 8 of the FIO, records relating to or connected with the defences forces or defence installations, or are ancillary to defence and national security, are exempt from the records that citizens may request access to under the FIO.

5.4 Prevention of Electronic Crimes Act 2016 ("PECA")

The Federal Investigation Agency (FIA) has been designated as the Investigation Agency under PECA.

6. PUBLICATION OF LAWS AND AGGREGATE DATA RELATING TO LAWFUL INTERCEPT AND COMMUNICATIONS DATA REQUESTS

Publication of laws

6.1 Constitution of Pakistan and the Freedom of Information Ordinance 2002 ("FIO")

As stated in paragraph 5.3 above, all citizens have the right to information held by public authorities that is on the public record, subject to certain restrictions and exemptions. Therefore, unless the information in question falls under one of these restrictions or exemptions, there is no legal authority for the government to prevent the publication of the laws to which operators of telecommunications networks and providers of telecommunications services licensed to operate in Pakistan ("Network Operators") are subject.

Publication of Aggregate Data

6.2 Official Secrets Act 1923 (the "OSA")

Under section 5 of the OSA, it is an offence for any person, who has in his possession or control information which has been entrusted to him in confidence by a public servant, to intentionally communicate such information to anyone who is not authorised to receive it.

Such disclosure of confidential information relating to lawful interceptions and communication data requests, including the aggregate number of them over a defined period of time (assuming that a Network Operator has such information), may constitute an offence under section 5.

6.3 Investigation for Fair Trial Act 2013 ("IFTA")

As stated in paragraph 1.4 above, interceptions made under IFTA are given lawful authority by a secret court process and are implemented by Network Operators operating under a duty of confidentiality. In some circumstances data relating to IFTA interceptions may, when used as evidence at trial, subsequently be included in the official records of the trial at the court in question.

6.4 Prevention of Electronic Crimes Act 2016 ("PECA")

Under section 53 of PECA, the FIA shall submit a half yearly report to both houses of the Parliament for consideration by the relevent Committee in camera, in respect of its activities, without disclosing identity information, in a manner as prescribed under PECA.

7. CYBERSECURITY

Pakistan is yet to create specific legislation that imposes obligations on companies to take measures to improve their IT security posture or perform other tasks of a defensive nature, such as to report any material breaches of their IT security to a regulator. The only provisions that are applicable in this regards are those contained within the Prevention of Electronic Crimes Act.

7.1 Prevention of Electronic Crimes Act 2016 ("PECA")

Section 41 PECA which relates to the "confidentiality of information" provides that notwithstanding any immunity granted under any other law for the time being in force, any;

(i) person including a service provider while providing services under the terms of a lawful contract or otherwise in accordance with the law; or

(ii) authorized officer,

who has secured access to any material or data containing personal information about another person, discloses such material to any other person, except when required by law, without the consent of the person concerned or in breach of a lawful contract with the intent to cause or knowing that he is likely to cause harm, wrongful loss or gain to any person or compromise the confidentiality of such material or data, shall be punished with imprisonment for a term which may extend to three years or with a fine which may extend to one million rupees or with both.

Note that the burden of proof of any defence put forward by an accused service provider or an authorized officer that he was acting in good faith shall be on the service provider or authorized officer in question.

Moreover, Section 48 PECA which relates to the "prevention of electronic crimes" states that the Federal Government and the Pakistan Telecommunications Authority ("PTA") hold the power to issue directives to be followed by the owners of designated information systems or service providers in the interest of preventing any offence under the PECA. Where an owner of the information system who is not a licensee of the PTA violates any directives issued to it in accordance with Section 48, they shall be guilty of an offence punishable, if committed for the first time, with a fine which may extend to ten million rupees and upon any subsequent conviction with imprisonment which may extend to six months or with a fine or with both. On the other hand, where the violation is committed by a licensee of the PTA, the violation shall be deemed to be a violation of the terms and conditions of the licensee's licence and shall be treated as such under the Pakistan Telecommunication (Re-organization) Act 1996.

According to Section 29(1) the Federal Government has designated the Federal Investigation Agency (the "FIA") as the investigatory agency for the purposes of investigating offences of PECA. Under Section 30, only an authorized officer of the FIA shall have the powers to investigate an offence.

The statutory provisions of the PECA that are regulated by the PTA include;

- Section 32 which concerns the retention of traffic data;
- Section 37 which regulates unlawful online content; and
- Section 48 which concerns the prevention of electronic crimes.

Any decision of the FIA or PTA can be appealed to the special designated courts under Section 47 of the PECA.

8. CYBERCRIME

8.1 Prevention of Electronic Crimes Act 2016 ("PECA")

The PECA also regulates, deals with, and penalises hacking and other forms of unauthorised activity relating to IT networks and systems. These may include commissioning DDoS attacks, inserting malware into IT systems, accessing IT systems using stolen credentials and so on.

The provisions of the PECA explicitly prohibit a wide range of activities, including the following:

Statutory Reference	Offence	Penalty
Section 3	Unauthorized access to an information system or data Described as, with dishonest intent, gaining unauthorized access to any information system or data	Fine which may extend to fifty thousand rupees and/or imprisonment for a term which may extend to three months
Section 4	Unauthorized copying or transmission of data Described as, with dishonest intent and without authorization, copying or otherwise transmitting or causing to be transmitted any data	A fine which may extend to one hundred thousand rupees and/or imprisonment for a term which may extend to six months
Section 5	Interference with an information system or data Described as, with dishonest intent, interfering with, damaging, causing to be interfered with or damaging any part or whole of an information system or data	A fine which may extend to five hundred thousand rupees and/or imprisonment which may extend to two years
Section 6	Unauthorized access to a critical infrastructure information system or data Described as, with dishonest intent, gaining unauthorized access to any critical infrastructure information system or data	A fine which may extend to one million rupees and/or imprisonment which may extend to three years
Section 7	Unauthorized copying or transmission of critical infrastructure data Described as, with dishonest intent, and without authorization copying or otherwise transmitting or causing to be transmitted any critical infrastructure data	A fine which may extend to five million rupees and/or imprisonment for a term which may extend to five years
Section 8	Interference with a critical infrastructure information system or data Described as, with dishonest intent, interfering with, damaging, causing to be interfered with or damaging any part or whole of a critical information system or data	A fine which may extend to ten million rupees and/or imprisonment which may extend to seven years
Section 10	Cyber terrorism Described as committing or threatening to commit any of the offences under Sections 6, 7, 8 or 9, where the commission or threat is with the intent to: (a) coerce, intimidate, create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or (b) advance inter-faith, sectarian or ethnic hatred; or (c) advance the objectives of organizations or individuals or groups prescribed under the law	A fine which may extend to fifty million rupees and/or imprisonment of either description for a term which may extend to fourteen years

Statutory Reference	Offence	Penalty
Section 15	Making, obtaining or supplying a device for use in an offence Described as producing, making, generating, adapting, exporting, supplying, offering to supply or importing for use any information system, data or device, with the intent for it to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under the PECA	(Without prejudice to any other liability that he may incur in this regards) a fine which may extend to fifty thousand rupees and/or imprisonment for a term which may extend to six months
Section 17	Unauthorized issuance of SIM cards etc. Described as selling or otherwise providing a subscriber identity module (SIM) card, re-usable identification module (R-IUM) or other portable memory chip designed to be used in cellular mobile or wireless phone for the purposes of transmitting information without obtaining and verifying the subscriber's antecedents in the mode and manner for the time being approved by the Authority	A fine which may extend to five hundred thousand rupees and/or imprisonment for a term which may extend to three years
Section 18	Tampering, etc. of communication equipment Described as unlawfully or without authorization changing, altering, tampering with or re-programing the unique device identifier of any communication equipment including a cellular or wireless handset and starting to use or market such a device for the purposes of transmitting and receiving information Note, a "unique device identifier" is an electronic equipment identifier which is unique to a mobile wireless communication device	A fine which may extend to one million rupees and/or imprisonment which may extend to three years
Section 19	Unauthorized interception Described as, with dishonest intent, committing unauthorized interception by technical means of; (a) any transmission that is not intended to be and is not open to the public, from or within an information system; or (b) electromagnetic emissions from an information system that are carrying data	A fine which may extend to five hundred thousand rupees and/or imprisonment of either description for a term which may extend to two years
Section 23	Malicious code Described as willfully and without authorization writing, offering, making available, distributing or transmitting malicious code through an information system or device, with the intention to cause harm to any information system or data resulting in the corruption, destruction, alteration, suppression, theft or loss of the information system or data	A fine which may extend to one million rupees and/or imprisonment for a term which may extend to two years

Statutory Reference	Offence	Penalty
Section 24	Cyber stalking Described as with the intent to coerce, intimidate or harass any person, using an information system, information system network, the Internet, a website, electronic mail or any other similar means of communication to– (a) follow a person or contacts or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person; (b) monitor the use by a person of the Internet, electronic mail, text message or any other form of electronic communication; (c) watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress in the mind of such person; or (d) take a photograph or make a video of any person and displays or distributes it without his consent in a manner that harms a person Where the victim of the cyber stalking activity committed is a minor	A fine which may extend to one million rupees and/or imprisonment for a term which may extend to one year Also note any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for the removal, destruction of or blocking of access to the information referred to in this section. The Authority, on receipt of such application, may pass such orders as deemed appropriate. The Authority may also direct any of its licensees to secure such information including traffic data A fine which may extend to ten million rupees and/or imprisonment of up to five years

In regards to the extraterritorial reach of cybercrime legislation in Pakistan, Section 42 PECA states that the Federal Government may upon receipt of a request for co-operation, extend such cooperation to any foreign government, 24 x 7 network, foreign agency or international organization or agency. This is only for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offence or obtaining expeditious preservation and disclosure of data by means of an information system or real-time collection of data associated with specified communications or interception of data under the PECA.

The Federal Government may also forward to a foreign government, 24 x 7 network, foreign agency or international agency or organization, any information obtained from its own investigations if it considers that the disclosure of such information might assist the other government, agency or organization etc., as the case be, in initiating or carrying out investigations or proceedings concerning any offence under the PECA. The Federal Government may also require the foreign government, 24 x 7 network, foreign agency or international agency to keep the information provided confidential or use it strictly for the purposes it is provided for.

Further, the Federal Government may send and answer requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

Where the Federal Government decides to provide the requested cooperation, the relevant requirements and safeguards provided under the PECA must be followed.

The Federal Government may however refuse to accede to any request made by a foreign government, 24 x 7 network, foreign agency, international organization or agency if:

(a) it is of the opinion that the request, if granted, would prejudice sovereignty, security, public order or other essential public interests of Pakistan;

(b) the offence is regarded by the Federal Government as being of a political nature;

(c) there are substantial grounds for believing that the request for assistance has been made for the purpose of prosecuting a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions or that that person's position may be prejudiced for any of those reasons;

(d) the request relates to an offence, the prosecution of which in the requesting State may be incompatible with the laws of Pakistan;

(e) the assistance requested requires the Federal Government to carry out compulsory measures that may be inconsistent with the laws or practices of Pakistan had the offence been the subject of an investigation or prosecution under its own jurisdiction; or

(f) the request concerns an offence which may prejudice an ongoing investigation or trial or the rights of its citizens guaranteed under the Constitution.

The PECA also requires the designated agency to maintain a register of requests received from foreign governments, 24 x 7 networks, foreign agencies or international organizations or agencies.

Law stated as at 22 February 2017

SERBIA – 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 Serbian law.

1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

1.1 Constitution of the Republic of Serbia (Official Gazette of the Republic of Serbia no. 98/2006, Ustav Republike Srbije) (the "Constitution")

Article 41 of the Constitution guarantees the confidentiality of letters and other means of communication, and provides that derogation from this right is allowed only if necessary to conduct criminal proceedings or to protect the security of the Republic of Serbia, in a manner stipulated by the law and by a decision of a competent court. Any such derogation must be for a specified period of time.

1.2 Electronic Communications Act (Official Gazette of the Republic of Serbia nos. 44/2010, 60/2013 and 62/2014, Zakon o elektronskim komunikacijama) (the "ECA")

Article 37, paragraph 2, subparagraph 17 and Article 127, paragraph 1 ECA oblige network operators and service providers to enable the lawful interception of electronic communications required by government agencies for the purpose of criminal investigations. Interceptions of electronic communications which reveal the content of a communication are allowed only for a limited period of time and on the basis of a court decision, if such interception is necessary to conduct criminal proceedings or for the protection of national security as per Article 126, paragraph 1.

The ECA does not specify which government agencies may request interception or the maximum duration of any interception carried out. However, since interception is allowed for the purposes of conducting criminal proceedings or for the protection of national security, only government agencies which operate in these areas (the police, the State Prosecutor, the Security-Intelligence Agency and the Military Security Agency (Proveriti na kraju) would be authorised to require interception in accordance with the ECA and the legislation specific to their activities (described further below), which also regulate the maximum duration of each interception.

Articles 37 and Article 127 provide that network operators and service providers have an obligation to enable the lawful interception of electronic communications. Article 127 obliges network operators and service providers to provide, at their own expense, the necessary technical and organizational conditions (equipment and software support) to enable the interception of electronic communications and to inform the Agency for Electronic Communications (the "Agency") about the interception. Article 126 paragraph 1 states that the interception of electronic communications through which the content of communication is disclosed is not allowed without consent of the user, except for a definite period of time based on a decision of the competent court and only where it is necessary for the conducting of criminal procedure or the protection of security of the Republic of Serbia, in a manner prescribed by law. The court decision should specify the government agency designated to conduct the interception.

Government agencies that conduct lawful interceptions are obliged to keep records of the interceptions and to keep these records as a secret pursuant to Article 127 paragraph 2. According to Article 127 paragraph 3 ECA, if a government agency which is authorised to intercept an electronic communication and is not able to do so without requiring assistance to access the premises, the electronic communications network, other instruments or the electronic communications equipment of the network operator or service provider, the obligation to keep records of the interception lies with the network operator or service provider. In both instances, under Article 126 paragraph 1, a court decision is required to authorise the interception.

1.3 Criminal Procedure Code (Official Gazette of the

Republic of Serbia nos. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 and 55/2014, Zakonik o krivičnom postupku) (the "CPC")

Article 161 CPC provides that interception and surveillance of electronic communications may be employed, as special investigation measures, in pre-formal and formal investigation stages of criminal proceedings, and ordered against a person suspected of committing or preparing a war crime, organized crime, cybercrime or one of various listed serious crimes (stated in Article 162, paragraphs 1, 2 and 3), if evidence of that crime cannot be collected in any other way, or if gathering evidence by regular investigatory measures would cause significant difficulties.

The order for interception is issued by the competent criminal court upon the request of the State Prosecutor for a period of three months with the possibility of an extension of three more months. In cases of war crimes and organized crime, this maximum six months period may be extended twice, each time for an additional three months as per Articles 166 and 167.

Article 168 provides that the interception may be performed by the police, the Security-Information Agency or the Military Security Agency. If during the interception the relevant government agency obtains information indicating that a person is using or has used another phone number or address, the interception may be extended to include that phone number or address also, by a decision of the director of that government agency, who will also notify the State Prosecutor. The State Prosecutor will subsequently file the request for an extension with the competent criminal court which will, under Article 169 either, render a new decision approving the extension or order the destruction of the materials collected.

1.4 Police Act (Official Gazette of the Republic of Serbia no. 6/2016, Zakon o policiji) (the "PA")

The PA authorises the police to intercept electronic communications if such interception is necessary to arrest or apprehend a person reasonably suspected of having committed an offence punishable with imprisonment of four or more years and for whom an international arrest warrant is issued, if the police cannot apprehend such a person by other means or when other means would involve disproportionate difficulties.

The request for interception is submitted by the director of the police and approved by the president of the Cassation Court or, in the absence of the president of the Cassation Court, by a judge of the Cassation Court authorised to rule on such a request. Each interception may last up to six months and may be extended by an additional six months.

Materials collected by an interception may not be used as evidence in criminal proceedings and must be submitted for destruction to the president of the Cassation Court or the authorised judge of that court immediately upon completion of the interception. In circumstances in which waiting for the court's approval might jeopardise a police investigation, the interception may be ordered by a decision of the director of the police, with prior written approval of the president of the Cassation Court or the authorised judge of that court. In such cases, the director of the police is obliged to submit to the court a written request for continued interception within 24 hours from obtaining prior approval. The court, under Article 60, will decide on the continuation or suspension of the interception within 72 hours of receipt of the request.

1.5 Security-Information Agency Act (Official Gazette of the Republic of Serbia nos. 42/2002, 111/2009, 65/2014 and 66/2014, Zakon o bezbednosno-informativnoj agenciji) (the "SIAA")

The SIAA provides for secret surveillance and recording of communications or surveillance of an electronic or any other address as special measures which may be employed against a person, group or organization that is reasonably suspected of undertaking or preparing activities which threaten the security of the Republic of Serbia. Such special measures may only be used pursuant to Articles 13 and 14 when the circumstances of the case indicate that the suspected activities could not be discovered, prevented or proved by other means, or that other means would involve disproportionate difficulties or serious danger. The SIAA does not define serious danger nor specify who should be in serious danger for these provisions to take effect.

Article 15 provides that secret surveillance must be requested by the director of the Security-Information Agency and ordered by the president of the Higher Court in Belgrade (the "President") or a judge of the special department of the Higher Court in Belgrade who handles cases of organized crime, corruption and other serious offences (the "Judge"). The interception may be ordered for a period of three months and, if necessary, may be extended up to three times, each time for a period of three months as per Article 15a.

If during the interception the Security-Information Agency obtains information indicating that the subject of the interception is using other means of communication, the director of the Agency may file a request for extension of the interception to include the discovered means of communications. If the President or Judge adopts this request, a new decision will be rendered approving the extension. If the request is rejected the collected materials must be destroyed as stipulated in Article 15b.

1.6 Military Security Agency and Military Intelligence Agency Act (Official Gazette of the Republic of Serbia nos. 88/2009, 55/2012 and 17/2013, Zakon o vojnobezbednosnoj agenciji i vojnoobaveštajnoj agenciji) (the "MSA")

Under the MSA, the Military Security Agency, which is in charge of security and counter intelligence protection of the Ministry of Defence and Military of the Republic of Serbia as per Article 5, is authorised under Articles 11 and 12, to secretly collect data as a special measure (including interception under the ECA) if this data cannot be collected by other means or if collection of this data by other means would cause disproportionate risk to

the lives and health of people and property, or disproportionate expense. Article 11 paragraph 2 further states that information may be collected for the purpose of preventing threats directed at the Ministry of Defence and the Military of the Republic of Serbia.

This measure can be applied on the basis of a written and reasoned decision of the Cassation Court in response to a request of the Director of the Military Security Agency and may be ordered for a period of six months, with the possibility of extension by an additional six months as per Articles 14 and 17.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Constitution of the Republic of Serbia (Official Gazette of the Republic of Serbia no. 98/2006, Ustav Republike Srbije) (the "Constitution")

With reference to Article 41 of the Constitution (described above), the Constitutional Court of Serbia has issued held that derogation from the confidentiality of "other means of communications" includes not only interception of communications which would reveal the content of communications, but also the collection of metadata. Consequently, the Constitution Court has confirmed its prior opinion that the limitation of the right to confidentiality of communication transferred by telecommunication networks may be done only on the basis of court decision (DecisionIUz-1218/2010 of the Constitutional Court of Serbia).

2.2 Electronic Communications Act (Official Gazette of the Republic of Serbia nos. 44/2010, 60/2013 and 62/2014, Zakon o elektronskim komunikacijama) (the "ECA")

According to Article 128 paragraph 2, network operators and service providers are obliged to disclose retained metadata to government agencies (the police, the State Prosecutor, the Security-Information Agency and the Military Security Agency) that obtain a court decision allowing them such access for a limited period of time and for the purpose of conducting criminal proceedings or national security.

According to Article 128 paragraph 6 and Article 129, network operators and service providers are obliged to retain (for a period of 12 months) data:

(a) tracing and identifying the source of a communication;

(b) identifying the destination of a communication;

(c) determining the beginning, duration and end of a communication;

(d) identifying the type of communication;

(e) identifying users' terminal equipment; and

(f) identifying the location of the users' mobile terminal equipment.

Network operators and service providers must retain customers' metadata for a period of 12 months and government agencies are only allowed to request access to such metadata.

Under Article 129, network operators and service providers must not retain the content of customer communications. Since however Article 126 and 127 allow the interception of electronic communications on the basis of a court decision, if such a court decision contains an order for the retention of the content of electronic communications, then network operators and service providers would be obliged to act upon it.

2.3 Criminal Procedure Code (Official Gazette of the Republic of Serbia nos. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 and 55/2014, Zakonik o krivičnom postupku) (the "CPC")

Under the CPC, computer data searches of processed personal data and other data may be employed as a special investigation measure covering the collection of metadata retained by a network operator or service provider for the pre-trial and investigation phase of criminal proceedings. These measures may be ordered in relation to a person suspected of committing or preparing a war crime, organized crime, cybercrime or one of the listed serious crimes, if evidence of that crime cannot be collected in any other way or if gathering evidence by regular investigation measures would cause significant difficulties as per Articles 161, 162 and 178.

Pursuant to Article 167, the order for a computer data search will be provided by the competent court, upon the request of the State Prosecutor, for a period of three months with the possibility of up to two extensions, each time for an additional three months

Under Article 180, this measure is implemented by the police, the Security-Information Agency, the Military Security Agency, the customs, tax and other state authorities, or legal entities vested with official authority.

2.4 Police Act (Official Gazette of the Republic of Serbia no. 6/2016, Zakon o policiji) (the "PA")

Under the PA, the police are authorised to obtain metadata relating to electronic communications if it is necessary for arresting or apprehending a person who is reasonably suspected of having committed an offence punishable with imprisonment of four or more years, and for whom an international arrest warrant is issued, if the police cannot apprehend such a person by other means or when other means would involve disproportionate difficulties.

The request for obtaining metadata relating to electronic communications is submitted by the Director of the police and approved by the President of the Cassation Court or, in the absence of the President of the Cassation Court, by an authorised judge of the Cassation Court, within 72 hours of the receipt of the request. As per Article 60, this measure may last up to six months and may be extended by an additional six months.

2.5 Security-Information Agency Act (Official Gazette of the Republic of Serbia nos. 42/2002, 111/2009, 65/2014 and 66/2014, Zakon o bezbednosno-informativnoj agenciji) (the "SIAA")

Under Article 13 and 14 SIAA, obtaining metadata may be ordered as a special measure when the metadata relates to the communications of a person, group or organization under reasonable suspicion of undertaking or preparing activities which threaten the security of the Republic of Serbia, and the circumstances of the case indicate that their activities may not be discovered, prevented or proved by other means or that other means would involve disproportionate difficulties or serious danger.

Article 15 stipulates that this measure must be ordered by the President of the Higher Court in Belgrade (the "President"), or a judge of the special department of the Higher Court in Belgrade who handles cases of organized crime, corruption and other serious offences (the "Judge"), upon the request of the Director of the Security-Information Agency. The measure may be ordered for a period of three months and if necessary may be extended up to three times, each time for a period of three months as per Article 15a.

If disclosed metadata indicates that an individual, group or organization is using other means of communication, the director of the Security-Information Agency may order an extension of the special measure and subsequently file a request for the extension of a measure in relation to the discovered means of communications. If the President or Judge adopts this request, he/she will render a new decision approving the extension. Where such a request is not adopted, the collected materials must be destroyed in line with Article 15b.

2.6 Military Security Agency and Military Intelligence Agency Act (Official Gazette of the Republic of Serbia nos. 88/2009, 55/2012 and 17/2013, Zakon o vojnobezbednosnoj agenciji i vojnoobaveštajnoj agenciji) (the "MSA")

As mentioned above, under Article 11 MSA, the Military Security Agency is authorised to undertake the secret collection of data as a special measure in certain circumstances. Secret electronic surveillance of electronic communications for the purpose of obtaining retained traffic data is a special measure requiring a written decision of the Cassation Court, requested by the Director of the Military Security Agency, and may be ordered for a period of six months, with the possibility of extension for an additional six months pursuant to Articles 14 and 17.

2.7 Technical Conditions

According to the Technical conditions for subsystems, devices, equipment and installations for mobile telecommunication networks no. 1-01-110-7/08 ("Mobile Technical Conditions"), the Technical conditions for subsystems, devices, equipment and installations for landline telecommunication networks no. 1-01-110-8/08 ("Landline Technical Conditions") and the Technical conditions for subsystems, devices, equipment and installations for internet network no. 1-01-110-19/08 ("Internet Technical Conditions") issued by the Electronic Communications Agency, network operators and service providers are obliged to remove their encryptions prior to delivery of the content of communications or metadata relating to communications to the competent government agencies (Section 2, Mobile and Landline Technical Conditions and Section 6, Internet Technical Conditions).

3. NATIONAL SECURITY AND EMERGENCY POWERS

3.1 Defence Act (Official Gazette of the Republic of Serbia, nos. 116/2007, 88/2009, 88/2009 and 104/2009, Zakon o odbrani) ("DA")

According to Article 73 paragraph 1 DA, in a state of emergency or a state of war, legal entities in the postal-telegraph-telephone sector and other carriers of telecommunications systems must prioritise the delivery of their services as specified by the Ministry of Defence. The Decision on establishing large technical systems significant for defence (Official Gazette of the Republic of Serbia, nos. 41/2014, 35/2015 and 86/2016) stipulates that Telenor d.o.o., as well as Telekom Srbija a.d, and VIP mobile d.o.o. are significant technical systems in the field of telecommunications which are required to adjust their systems to the needs of the defence system in Serbia.

Article 202 of the Constitution allows for the introduction of measures which would provide derogation from the general protection given to the confidentiality of letters and other means of communication and the protection of personal data (under Article 41 of the Constitution) in a state of emergency or war. Government agencies may, on the basis of such measures, require access to a network operator's or service provider's customer communications data and/or network without adhering to the procedure prescribed for obtaining these data in regular circumstances; that is, without presenting a court decision authorizing the interception of the electronic communications or access to the retained data.

Measures providing for derogation from Article 41 of the Constitution are adopted by the National Assembly or, if the National Assembly is not in a position to convene, by government decree with the President of the Republic as a co-signatory in the case of a national emergency (as per Article 200, paragraph 6 of the Constitution) or by the President of the Republic together with the President of the National Assembly and the Prime Minister in the case of a state of war (as per Article 201, paragraph 4 of the Constitution).

Measures providing for derogation from Article 41 of the Constitution in a state of emergency are effective for a maximum of 90 days, with the possibility of extension under the same terms. Measures providing for derogation from Article 41 of the Constitution in a state of war may continue as long as necessary, as decided by the National Assembly, or the government, if the National Assembly is not in a position to convene.

3.2 Police Act (Official Gazette of the Republic of Serbia no. 6/2016, Zakon o policiji) (the "PA")

In accordance with Article 60, in emergency situations, the disclosure of metadata relating to electronic communications may be ordered by a decision of the director of the police, with prior written approval of the President of the Cassation Court or, in the absence of the President of the Cassation Court, by an authorised judge of the Cassation Court, in which case the Director of the police is obliged to submit a written request to the Court allowing the continued collection of metadata within 24 hours of obtaining prior approval.

3.3 Military Security Agency and Military Intelligence Agency Act (Official Gazette of the Republic of Serbia nos. 88/2009, 55/2012 and 17/2013, Zakon o vojnobezbednosnoj agenciji i vojnoobaveštajnoj agenciji) (the "MSA")

In emergencies, and particularly in cases of domestic and international terrorism, secret collection of data may be ordered by a decision of the Director of the Military Security Agency, with the interim prior approval of a judge of the Court of Cassation. The decision will subsequently be assessed in more detail and the judge will either grant a continuation of the measure or terminate the measure within 24 hours of its commencement as per Article 15.

4. CENSORSHIP

4.1 Enforcement and Security Act(Official Gazette of the Republic of Serbia, nos. 106/2015 and 106/2016, Zakon o izvršenju i obezbeđenju) ("ESA")

There is no provision which explicitly regulates censorship and authorises government agencies to request censorship of customer communications. However, network operators and service providers would be obliged to censor customers' communication pursuant to the ESA, if such order were given by a competent court in the form of an interim measure or in the form of a final court decision.

4.2 Electronic Commerce Act (Official Gazette of the Republic of Serbia, nos. 41/2009 and 95/2013, Zakon o elektronskoj trgovini)

Based on the request of the person whose rights are threatened, the court may decide under Article 21a paragraph 1 to limit the provision of the informatics society service, if that person can prove that the breach exists and if the person can prove that irreparable damage may occur. All service providers who transfer, store or provide access to data to which this measure is referred to, are obliged to act in accordance with such a court decision under Article 21a paragraph 2.

4.3 Electronic Communications Act (Official Gazette of the Republic of Serbia nos. 44/2010, 60/2013 and 62/2014, Zakon o elektronskim komunikacijama) (the "ECA")

Article 127 paragraph 3, prohibits network operators and service providers from publishing records on requests received for an interception which contain data identifying an authorised person who conducted the interception, the decision which provided the legal basis for interception and the date and time of the interception.

5. OVERSIGHT OF THE USE OF POWERS

5.1 Judicial Oversight

Interception of electronic communications conducted by all government agencies authorised to undertake such interception and the retention of the content of electronic communications is overseen by the competent court which ordered the measure and monitors its enforcement (Article 126, paragraph 1 and Article 128, paragraph 2 ECA; Articles 166 and 286 CPC; Article 60, paragraph 2 PA; Articles 15 and 16 SIAA; Articles 14 and 15 MSA). If the materials obtained by interception were not collected in accordance with the prescribed procedure, the competent court will order their destruction (Article 163 CPC; Article 15b SIAA; Article 15 MSA).

5.2 Electronic Communications Act (Official Gazette of the Republic of Serbia nos. 44/2010, 60/2013 and 62/2014, Zakon o elektronskim komunikacijama) (the "ECA")

The ECA contains provisions concerning the general oversight of network operators' and service providers' operations by the Agency for Electronic Communications (the "Agency") and the Inspectorate of the Ministry of Trade, Tourism and Telecommunications (the "Inspectorate").

At the request of the Agency, network operators and service providers are obliged to submit information on the protection of customers' personal data and privacy as per Article 41; to correct irregularities in its technical and organizational settings (enabling interception) identified by the Agency; and to inform the Inspectorate if a network operator or service provider does not comply with its request in accordance with Article 131.

Under Articles 132 and 134 paragraph 1, subparagraph 6, the supervision of network operators and service providers is also conducted by the Inspectorate. The Inspectorate is authorised to order a network operator or service provider to remedy irregularities, oversights or omissions in its work within a given period of time as per Article 135 paragraph 1, subparagraph 1.

Under Articles 132 and Article 134 paragraph 1, subparagraph 6, the Ministry of Trade, Tourism and Telecommunications also monitors network operators' and service providers' assistance in implementing interception capabilities. The Ministry of Trade, Tourism and Telecommunications is authorised to order network operators and service providers to implement such capabilities within a given period of time and to temporarily suspend their activities if they do not comply as per Article 135, paragraph 1, subparagraphs 1 and 3.

Network operators, service providers and government agencies are obliged to submit records in relation to requests received to access retained data in the preceding year on 31 January of each year to the Commissioner for Personal Data Protection.

The Commissioner is authorised under Articles 44, 45 and 56 PDPA to order certain measures if the data processing conducted was not in accordance with the law.

5.3 Police Act (Official Gazette of the Republic of Serbia no. 6/2016, Zakon o policiji) (the "PA")

According to Article 225, police activities are generally supervised by a special department of the Ministry of Police – the Division of Internal Control, which monitors the legality of police work, especially with regards to the respect and protection of human rights in the performance of police tasks and applying police powers.

5.4 Military Security Agency and Military Intelligence Agency Act (Official Gazette of the Republic of Serbia nos. 88/2009, 55/2012 and 17/2013, Zakon o vojnobezbednosnoj agenciji i vojnoobaveštajnoj agenciji) (the "MSA")

Article 57 provides for internal control of the Military Security Agency, conducted by the Division of Internal Control of the Military Security Agency. There is also political supervision over the work of the police, the Security–Information Agency and the Military Security Agency by the National Assembly and the government as per Article 17 SIAA and Article 57 MSA.

5.5 Constitution of the Republic of Serbia (Official Gazette of the Republic of Serbia no. 98/2006, Ustav Republike Srbije) (the "Constitution")

According to Articles 168 and 170, the Constitutional Court of Serbia, which is authorised to assess constitutionality and legality of laws and other general acts, may find that a measure of derogation from confidentiality of letters and other means of communication and the protection of personal data introduced during a state of war or emergency is unconstitutional.

5.6 Law on Constitutional Court of Serbia ("Official Gazette of the Republic of Serbia, nos. 09/2007, 99/2011, 18/2013 and 40/2015, Zakon o ustavnom sudu)

Network operators and service providers may file a constitutional appeal against a decision of a government agency as an individual act which violates Constitutional guarantees, when other legal remedies have been exhausted or are not prescribed or where the right to their judicial protection has been excluded by law as per Articles 82 and 83.

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

There is no law prohibiting the publication of any of the laws mentioned in this report or any description of the powers set out in any of those laws.

6.1 Electronic Communications Act (Official Gazette of the Republic of Serbia nos. 44/2010, 60/2013 and 62/2014, Zakon o elektronskim komunikacijama) (the "ECA")

Article 127 paragraph 3 ECA prevents network operators and service providers from publishing records of requests for interception or access to metadata that provide information on: the identity of the persons conducting the interception or who gained access to the metadata, the identity of the people whose communications were intercepted or whose metadata was accessed, the purpose of the interception or access, or the time and place of the interception or access.

This would not, however, prevent network operators or service providers publishing aggregate data on the number of requests to intercept communications for example, provided that none of the above information is included in this publication.

7. CYBERSECURITY

7.1 Information Security Act ("Official Gazette of the Republic of Serbia", no. 6/2016, Zakon o informacionoj bezbednosti) (the "ISA")

The ISA regulates the measures that may be taken (i) by legal entities in relation to their management and use of information-communication systems ("ICT Systems") and (ii) by the competent authorities responsible for the implementation of protective measures, to protect against the risk of cybersecurity breaches. Article 7 additionally regulates the area of crypto-security and the use of protective measures against Compromising Electromagnetic Emanations. The use of an electronic communications network by an operator of telecommunication services falls within the ISA's definition of an "ICT System".

Pursuant to Article 6, operators of ICT Systems related to electronic communications are defined as operators of essential services who are obliged to implement measures to ensure the protection of their ICT Systems. Article 7 goes on to provide 28 examples of such protective measures, one of which includes the measures to be taken against the unauthorised access to information in a computer system i.e. by preventing individuals knowingly sending computer viruses or otherwise attacking computer systems. These measures are regulated in detail by the Rulebook which more closely regulates the measures that may be taken to protect ICT Systems of special importance ("Official Gazette of the Republic of Serbia", no. 94/2016) (the "Rulebook").

Operators of essential services that use ICT Systems are also obliged to implement their own internal policies on security of their ICT Systems. Under Article 8, these policies should define the protective measures that are to be implemented, the principles and procedures for achieving and maintaining the adequate level of security of the ICT System and the duties and responsibilities related to the security and resources of the ICT System. Note that the exact content of this internal policy is also more particularly detailed in the Rulebook referred to above.

Each operator of essential services that uses ICT Systems must appoint an internal Computer Emergency Response Team (a "CERT") which is registered as an individual CERT with the

Regulatory Agency for Electronic Communications and Postal Services" (the "RATEL").

The RATEL performs the function of a national CERT. Operators of essential services are obliged to notify the RATEL of any cybersecurity incidents or attacks suffered by their ICT Systems that may have a significant impact on the security of the information they hold. The Rulebook provides further detail on the type of incidents that operators of ICT Systems of essential services must report. These include:

(a) incidents that lead to interruption or significant difficulties in continuing the performance of their activities;

(b) incidents that affect a large number of users;

(c) incidents that lead to interruption or significant difficulties in continuing the performance of the activities of other ICT Systems of special importance or public safety;

(d) incidents that lead to interruption or significant difficulties in continuing the performance of activities that could affect a significant part of the territory of the Republic of Serbia; and

(e) incidents that lead to unauthorized access to protected data which if published may jeopardize the rights and interests of persons to whom such data is related to.

To report a cybersecurity breach to the RATEL, the operator must make their report in writing within one day of its occurrence. If the incident relates to secret data, the operator is put under a further obligation to follow the rules related to data secrecy.

It is also important to note that the state body that is authorized to regulate the security of ICT Systems pursuant to Article 4 is the Ministry of Information Security which makes up part of the Ministry of Trade, Tourism and Telecommunications. Under Article 28 control over the compliance with the ISA is conferred upon the inspectors of information security, who are part of the Ministry.

The inspectors of information security are authorized to order operators of ICT Systems to correct any established irregularities and to prohibit any further use of their processes and technical means which jeopardize or undermine the information security of their ICT Systems. The inspector`s control is governed by the provisions of the ISA and the Inspection Control Act ("Official Gazette of the Republic of Serbia", no. 36/2015, Zakon o inspekcijskom nadzoru) (the "ICA"), which authorizes inspectors of information security to inspect the business records, business premises, objects, equipment and other means of work of the inspected legal entity.

The ISA does not contain an explicit provision that provides insight into which of the relevant authorities, the RATEL or the Ministry for Trade, Tourism and Telecommunications, would (if necessary) access an operator's telecommunications infrastructure to enhance its resilience against a cybersecurity attack. However, Articles 11 and 21 do illustrate the division of responsibility between these two authorities.

According to Article 14, the RATEL, as the acting national CERT, is responsible for monitoring and advising operators of ICT Systems of essential services, particularly when receiving reports concerned with the occurrence of a cybersecurity incident.

If the reported incident is of public interest, the RATEL may order public disclosure. Moreover, if the incident is related to crimes prosecuted ex officio, the RATEL shall inform the competent Public Prosecutor`s Office and/or the Ministry of Interior. If the incident alternatively or additionally involves a violation of personal data, the RATEL must report the incident to the Commissioner for Protection of Personal Data.

Therefore, whilst the ISA does not contain any provision which per se limit an individual's right to privacy and right to fair trial, the inspectors of the Ministry of Trade, Tourism and Telecommunications are provided with a prescribed level of access to a telecommunications infrastructure, particularly if it becomes necessary to establish whether the legal entity has implemented the required protective measures. Moreover, as mentioned previously, if the cybersecurity breach concerns secret or personal data, the reporting obligations of the operators of the ICT Systems and the corresponding prerogatives of the RATEL should be conducted in accordance with the general rules on data protection and data secrecy. Any failure to do so could raise the question of a violation of privacy rights.

Where a legal entity and its authorized representatives fail to comply with the ISA in the following ways:

- by failing to enact an internal regulation on security of its ICT System;
- by failing to apply the measures defined in its internal regulation on security of its ICT System;
- by failing to control the compatibility of the implemented measures with those provided by their own internal regulation on security of its ICT System; or
- by failing to comply with an order of an inspector for information security,

the breach will be punishable with a fine between RSD 50,000.00 and RSD 2,000,000.00 for the legal entity and a fine between RSD 5,000.00 and 50,000.00 for its authorized representatives.

Furthermore, pursuant to Articles 30 and 31, failure to report incidents related to ICT Systems to the RATEL is also a misdemeanor punishable with a fine between RSD 50,000.00 to RSD 500,000.00 for the legal entity in breach and RSD 5,000.00 to RSD 50,000.00 for its authorized representatives.

RATEL and the Ministry for Trade, Tourism and Telecommunications inspectors are both authorized to initiate misdemeanor proceedings.

In establishing the liability for misdemeanour under the ISA,

the court proceedings are conducted in accordance with the Misdemeanours Act ("Official Gazette of the Republic of Serbia", nos. 65/2013, 13/2016 and 98/2016, Zakon o prekrsajima) (the "MA") which under Article 258 provides that an appeal may be filed against the decision of the first instance misdemeanour court to the second instance misdemeanour court.

The enforcement of the final decision of the misdemeanor court is enforced by the court and/or public bailiffs in accordance with the provision of the Enforcement and Security Act ("Official Gazette of the Republic of Serbia nos. 106/2015 and 106/2016, Zakon o izvrsenju i obezbedjenju) (the "ESA").

The ISA does not prescribe a special appeal mechanism for individuals who are aggrieved by a decision taken by the RATEL or inspectors of the Ministry for Trade, Tourism and Telecommunications. However, since both the RATEL and inspectors of information security are administrative bodies of the Republic of Serbia, the general rules of the appeal process in administrative proceedings are applicable.

8. CYBERCRIME

8.1 Criminal Code of the Republic of Serbia (Official Gazette of the Republic of Serbia, nos. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013 and 108/2014, Krivični Zakonik Republike Srbije) (the "CC")

The CC recognizes the following eight cybercrimes:

Statutory Reference	Offence	Penalty
Article 298	Damaging Computer Data and Programs Described as without authorisation deleting, altering, damaging, concealing, or otherwise making unusable a computer data or program If the offence results in damages exceeding four hundred and fifty thousand dinars If the offence results in damages exceeding one million five hundred thousand dinars	Fine or imprisonment up to one year and the seizure of any equipment or devise used in the commission of the offence Imprisonment of three months to three years and the seizure of any equipment or devise used in the commission of the offence Imprisonment of three months to five years
Article 299	Computer Sabotage Described as entering, destroying, deleting, altering, damaging, concealing or otherwise making unusable computer data or programs or damaging or destroying a computer or other equipment used for electronic processing and transferring of data, with the intent to prevent or considerably disrupt the procedure of its electronic processing and transferring of data that is of importance to public services, governmental authorities, enterprises or other entities	Imprisonment of six months to five years
Article 300	Creating and Introducing Computer Viruses Described as making a computer virus with the intent to introduce it into another's computer or computer network Where the above offence causes damage	Fine or imprisonment up to six months and the seizure of any equipment or devise used in the commission of the offence Fine or imprisonment up to two years and the seizure of any equipment or devise used in the commission of the offence
Article 301	Computer Fraud Described as entering incorrect data, failing to enter correct data or otherwise concealing or falsely representing data and thereby affecting the results of the system's electronic processing and transferring of data with the intent to acquire for himself or another unlawful material gain and thus causing material damage to another person or entity If the offence results in the acquisition of material gain exceeding four hundred and fifty hundred thousand dinars If the offence results in the acquisition of material gain exceeding one million five hundred thousand dinars Where the offence is committed with malicious mischief	Fine or imprisonment up to three years Imprisonment of one to eight years Imprisonment of two to ten years Fine or imprisonment up to six months

Statutory Reference	Offence	Penalty
Article 302	Unauthorised Access to Computer, Computer Network or Electronic Data Processing Described as, by circumventing protective measures, accessing a computer or computer network without authorisation, or accessing electronic data processing without authorisation Where an individual records or uses the data obtained in the manner described above Where the offence specified results in the hold-up or serious malfunction of electronic processing and transferring of data of a network, or other grave consequences have resulted	Fine or imprisonment up to six months Fine or imprisonment up to two years Imprisonment up to three years
Article 303	Preventing or Restricting Access to Public Computer Network Described as without authorisation preventing or hindering access to a public computer network If the offence is committed by an official in discharge of their duty	Fine or imprisonment up to one year Punished by imprisonment up to three years
Article 304	Unauthorised Use of Computer of Computer Network Described as using a computer service or computer network with the intent to acquire unlawful material gain for himself or another	Fine or imprisonment up to three months (Note that prosecution for this offence shall be instigated by a private action)
Article 304(a)	Production, Obtaining and Distribution of means for Committing Crimes against the Safety of Computer Data Described producing, selling, obtaining for use, import, distribute or giving to use in another way: i) computers and computer programs projected or at first for the purposes of committing any crime prescribed in articles 298 - 303; ii) computer codes or similar data by which it might be accessed to computer system in whole or any of its parts with the aim to be used for the purposes of committing any crime prescribed in articles 298 - 303. If the person owns means mentioned in previous paragraph with the aim to be used for the purposes of committing any crime prescribed in articles 298 - 303.	Imprisonment between six months and three years and the seizure of any device used in the commission of the offence Fine or imprisonment up to one year and the seizure of any device used in the commission of the offence

The agencies responsible for the prosecution of cybercrimes are the Department of the Public Prosecutor's Office for Cybercrime, the Serbian police forces (particularly the unit of the Ministry of Interior specialized in investigating cybercrimes) and the criminal courts of the Republic of Serbia.

The police is authorized to investigate cybercrimes in accordance with the provisions of the Police Act ("Official Gazette of the Republic of Serbia", no. 6/2016, Zakon o policiji) (the "PA") and the Criminal Procedure Code ("Official Gazette of the Republic of Serbia", nos. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 and 55/2014, Zakonik o krivicnom postupku) (the "CPC") upon obtaining instructions from the Republic Prosecutor`s Office. In principle, the PA and the CPC require court approval prior to the undertaking of any of the investigatory measures that could violate an individual's right to privacy. These provisions additionally contain provisions that guarantee an individual's right to a fair trial.

Under the CC, the criminal law of Serbia shall also apply to foreigners who commit a criminal offence against Serbia or one of its citizen outside the territory of Serbia, if they are found on the territory of Serbia or if extradited to Serbia. Criminal prosecution shall be undertaken when criminal offences are also punishable by the law of the country where committed. If the law of the country where the offence was

committed does not provide for criminal prosecution for such an offence, criminal prosecution may be undertaken only with the permission of the Republic Public Prosecutor.

The criminal legislation of Serbia shall additionally apply to a foreigner who commits a criminal offence abroad against a foreign state or foreign citizen, when such offence is punishable by five years' imprisonment or a heavier penalty, pursuant to laws of the country where the crime was commissioned, if this individual is found on the territory of Serbia and is not extradited to the foreign state. If at the time of commission of the act, it was not punishable in the country where the crime was committed, but the act is considered a criminal offence under general legal principles of international law, prosecution may be undertaken in Serbia following the permission of the Republic Public Prosecutor, regardless of the law of the country where the offence was committed.

Under Articles 9 and 10 CC, criminal prosecution shall not be undertaken if:

- the offender has fully served the sentence to which he was convicted abroad;
- the offender was acquitted abroad by final judgment, the statute of limitations has expired in respect of the punishment, or the offender was pardoned;
- if dealing with an offender of unsound mind, a relevant security measure was enforced abroad; or
- for the prosecution of a criminal offence under foreign law, a motion of the victim was required and such motion was not filed

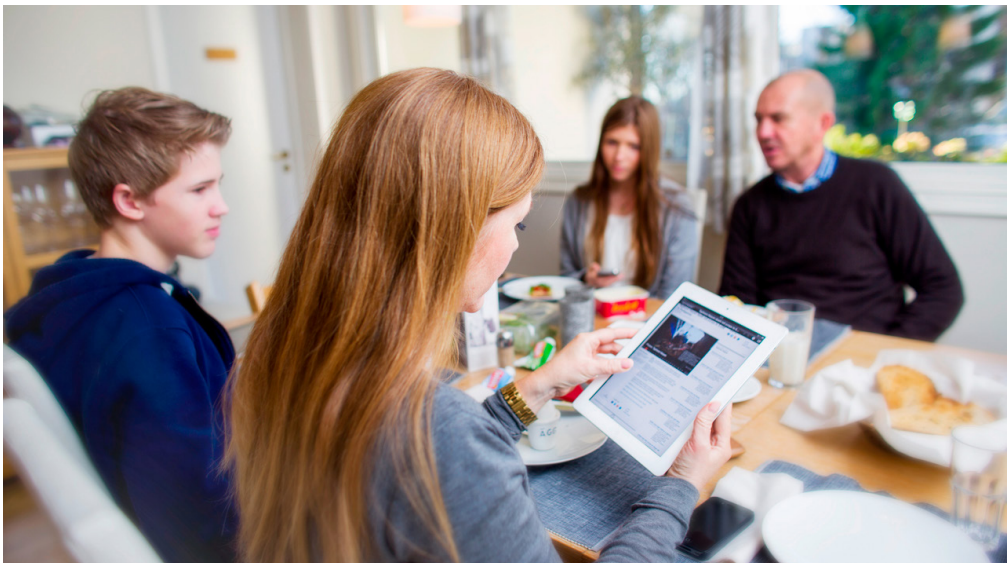
Note that Article 432 of the Criminal Procedure Code provides that appeals may be filed against the decision of the first instance court to a court of second instance.

Law stated as at 20 February 2017.

SWEDEN – 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 Swedish law.



1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

1.1 Electronic Communications Act 2003 (2003:389) (lag (2003:389) om elektronisk kommunikation) (the "ECA")

According to chapter 6, section 17, it is prohibited to intercept content data or monitor metadata associated with an electronic message.

However, under chapter 6, sections 19 and 21, network operators and service providers are obligated to:

(a) conduct their business and adapt and construct their network in a manner that enables the execution of court orders for the secret interception of electronic communications messages; and

(b) conduct their business in a manner that enables the execution of such court orders for secret interception without disclosure of such interceptions.

The content of an intercepted message must be made available in a form that can be easily processed by the government agency requesting the interception.

Chapter 6, section 19(a) requires network operators and service providers that own cables through which electronic signals are transmitted over the Swedish border, to transmit such signals to certain interaction points chosen by the network operator or service provider. The network operator or service provider must notify the National Defence Radio Establishment (Försvarets radioanstalt) (the "NDRE") of the location of these selected interaction points. Obligation with this requirement allows the Inspection of Defence Intelligence (the "IDI") to gain technical access to the electronic signals at the interaction points in accordance with the Defence Signals Intelligence Act (2008:717) (lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet) (the "DSIA"). The IDI is then able to transmit some of the signals on to the NDRE, in accordance with their obligations under the DSIA.

In accordance with sections 5, 5(a) and 12 DSIA, the NDRE must present a court order from the Defence Intelligence Court mandating the monitoring of the electronic signals in question. The IDI does not however need to present a court order to require access to all the electronic signals passing through the interaction points. Consequently, the relevant network operator or service provider is obliged to give the IDI access to the cable-based electronic signals that pass through an interaction point, without the need for a court order or warrant.

The NDRE is responsible for the actual construction of the interaction point, for securing technical access to the signals at the interaction point and for further transmitting them to its own systems. While the network operator or service provider is obliged to bear the costs associated with the transmission of the signals to the interaction point, the NDRE bears the costs associated with the operation of the interaction point.

These requirements fall under the remit of defence intelligence conducted to support the Swedish foreign, security and defence policies and for mapping external threats to the country.

Chapter 6, section 19(a) also obliges any network operator or service provider that carries signals over the Swedish borders through cables to disclose to the NDRE any information in its possession that makes it easier for the NDRE to manage and intercept the signals accessed at an interaction point, for example, the title, architecture, bandwidth, or direction of the connections and the type of signalling. The obligation applies to all network operators or service providers that carry

cross-border signals i.e. not only to the network operators and service providers that own the cables.

1.2 Code (1942:740) of Judicial Procedure (Rättegångsbalk (1942:740) (the "CJP")

Pursuant to chapter 27, section 21, the general obligation for network operators and service providers to provide interception assistance is qualified by the requirement that the requesting government agency first obtains a court approval authorising the interception. The request must be submitted to the competent court by a public prosecutor. According to chapter 27, section 18, a request for interception may only be granted in investigations relating to certain serious crimes. In this context, "serious crimes" include crimes for which the prescribed minimum penalty is imprisonment for two years or more and offences such as sabotage, arson, espionage, and terrorism.

In addition, a court approval will only be granted if the conditions set out in chapter 27, section 20 are fulfilled. Section 20 states that the use of interception must be of exceptional importance for the purpose of facilitating the criminal investigation in question. The court approval may only concern a particular number, address or the electronic communications equipment possessed by an individual who can reasonably be suspected of committing the crime under investigation. It may also concern another individual but only if there are particular reasons to believe that they will be contacted by the suspect.

According to chapter 27, section 21(a), if the public prosecutor responsible for the investigation deems that awaiting the court approval would result in a delay of material importance to the investigation, the public prosecutor may himself, without first obtaining a court approval, authorise an interim order for the secret interception. In such cases, the public prosecutor should inform the court of its decision, following which the court must promptly evaluate the interim order. If the court does not find reasons to support the decision, it must revoke the earlier decision, in which case no information collected under the interim order may be used in the investigation, if such information is detrimental to the person concerned.

Under chapter 27, section 22, it is prohibited to intercept communications involving information entrusted to certain individuals in their professional capacity. Such individuals are those who, according to chapter 36, section 5, are prohibited from disclosing information mentioned in the conversation. Examples of such individuals include advocates, physicians and freelance journalists (in relation to their sources).

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Electronic Communications Act 2003 (2003:389) (lag (2003:389) om elektronisk kommunikation) (the "ECA")

According to chapter 6, section 20, all data relating to customer communications, including metadata and content data, are confidential and may not be disclosed to anyone other than the participants of the relevant communication.

However, according to chapter 6, section 22, confidentiality does not apply in the following situations, where the network operator or service provider must disclose:

- customer subscription details, upon request from any government agency, where they are needed for serving a person in accordance with the Service of Process Act (2010:1932) (delgivningslag (2010:1932)), if it could be expected that the person sought to be served is hiding or if there otherwise are exceptional reasons for such disclosure;
- customer subscription details, which relate to a suspected crime, upon request from the Public Prosecution Authority (Åklagarmyndigheten), the Police Authority (Polismyndigheten), the Swedish Security Service (Säkerhetspolisen) or any other government agency investigating a suspected crime;
- customer subscription details relating to a customer and other information relating to a specific electronic message, including information about the geographic area in which the relevant communication equipment is or has been situated, upon request from the Police Authority. The Police Authority can only make such a request to assist in the search for a person who has gone missing in circumstances which suggest their life is in danger or that they are at serious risk of harm;
- customer subscription details, upon request by the Enforcement Authority (Kronofogdemyndigheten), if needed in an enforcement process (meaning in the collection of debts or actions related to such enforcement) and the Enforcement Authority deems such information to be of material importance to the processing of a certain matter;
- customer subscription details, upon request by the Tax Agency (Skatteverket), in the event such information is of material importance to the processing of any matter relating to the calculation of tax owed, payment of tax-related charges or any matter relating to the correct registration of an address or domicile in accordance with the National Registration Act (1991:481) (folkbokföringslag (1991:481));
- customer subscription details, upon request from the Police Authority, if such information is needed for providing notification, obtaining information or identifying persons in relation to accidents or casualties, or when investigating such accidents or casualties, or when the Police Authority leave a person aged under 18 years old to the care of the social services in accordance with section 12 of the Police Act (1984:387) (polislag (1984:387));
- customer subscription details, upon request by the Police Authority or the Public Prosecution Authority, if such authority determines such information is necessary in order for the authority to be able to inform a guardian in accordance with Section 33, of the Act (1964:167) on Juvenile Criminals (lagen (1964:167) om särskilda bestämmelser om unga lagöverträdare); and

- customer subscription details and other information relating to a specific electronic message, upon request by a regional emergency service centre (regional alarmeringscentral) in accordance with the Act (1981:1104) on Regional Emergency Service Centres (lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler).

A request under section 22 ECA does not require a court approval or any particular decision by the relevant government agency.

Under chapter 6, section 16(c) ECA, a government agency may only request metadata retained by a network operator or service provider under chapter 6, section 16(a) in the following situations:

(a) where a network operator or service provider must, upon request from the Public Prosecution Authority, the Police Authority, the Swedish Security Service or any other government agency, in connection with an investigation of a crime, disclose customer subscription details pursuant to chapter 6, section 22;

(b) where, pursuant to a court order sought by a public prosecutor under chapter 27, section 21 CJP, network operators and service providers are, pursuant to chapter 27, section 19 CJP, required to disclose to the Police Authority, the Swedish Security Service or the Customs Agency (Tullverket) the following metadata (as detailed in the court order):

(i) information on messages which have been transmitted across an electronic telecommunications network or which have been transmitted to or from a telephone number or other address;

(ii) information on what electronic communication devices have been present within a certain geographic area; and

(iii) Information concerning in what geographic area a certain electronic communication device is or has been present.

(iv) According to chapter 6, sections 16(a) to 16(f), a network operator or service provider must retain customer subscription details and other information relating to a certain electronic message, which are necessary to track and identify:

(a) the source of the communication;

(a) the ultimate destination of the communication;

(a) the date, time and duration of the communication;

(a) the type of communication;

(a) the communication equipment; and

(a) the localisation of mobile communication equipment at the commencement and end of the communication.

Network operators and service providers are also obliged to retain data relating to failed calls or connections, in relation to which the network operator or service provider shall retain the data generated or processed.

The specific information which should be retained by a network operator or service provider is further clarified in sections 38 to 43, of the Ordinance (2003:396) on Electronic Communication (förordning (2003:396) om elektronisk kommunikation) (the "OEC"). In addition, under section 44 OEC, the Swedish Post and Telecommunication Authority (Sw. Post- och telestyrelsen) (the "PTA") may stipulate more detailed requirements relating to the storage of data.

The PTA, under exceptional circumstances, may also create exemptions from the obligation to retain data as per chapter 6, section 16(b) ECA. In such event, the PTA will consult with the Public Prosecution Authority, the Police Authority and the Swedish Security Service as obligated to do so by section 45 OEC.

According to chapter 6, section 16(d) ECA, data retained in accordance with chapter 6, section 16(a) ECA, must be retained for six months from the date the communication ended. After this period, the network operator or service provider must permanently delete the retained data.

It should be noted that chapter 6, sections 16(a) to 16(f), implement Directive 2006/24/EC of the European Parliament and of the Council (the "Data Retention Directive"), which on 8 April 2014 was declared invalid by the Court of Justice of the European Union (the "ECJ"). As a consequence, the validity of the data retention obligations of network operators and service providers described above was contested by certain network operators and service providers operating in Sweden. After the Administrative Court of Stockholm, on 13 October 2014, upheld the Swedish implementation of the Data Retention Directive as lawful, the case was appealed and subsequently referred to the ECJ.

On 21 December 2016 the ECJ delivered a judgement striking down chapter 6, sections 16(a) to 16(f) ECA as inconsistent with provisions of the Charter of Fundamental Rights of the European Union (joined Cases C-203/15 & C-698/15). In summary, the ECJ concluded that the Charter of Fundamental Rights precluded such legislation as it provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication. However, according to the ECJ, EU Member States are allowed to adopt laws to retain traffic and location data so long as the purpose of the legislation is to fight serious crimes, and the retention of the data is proportionately limited with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period. Accordingly, what has been set out above regarding chapter 6, section 16(a) to 16 (f) ECA must be considered with some caution.

The Swedish legislator has not yet reacted to this ECJ judgment and thus the state of the law in this area is uncertain. Moreover, it is important to note that the ECJ judgment may also affect other legislative acts and the legal position should therefore be reevaluated accordingly.

2.2 Act (2012:278) on Collection of Data in Electronic Communication in the Crime Combatting Authorities' Intelligence Services (lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet) (the "IEUK")

Following a decision from the Police Authority, the Swedish Security Service or the Customs Agency, made by a duly authorized representative (meaning the head of the agency or a person to which the head of the agency has delegated the right), a network operator or service provider must, in accordance with section 1, disclose the metadata outlined under chapter 27 CJP summarised in paragraph 2.1(b) of this report above.

According to section 2, information may only be collected if:

(a) the collection is of particular importance in order to prevent or discover criminal activities, which involves any crime that is punishable with no less than two years imprisonment; and

(a) the reasons for the collection outweigh the interests of the person in relation to which the measure is targeted.

A court order will be required in accordance with chapter 27, section 21 CJP (as described above).

In this context, please note the information regarding the ECJ judgement delivered in December 2016 set out under section 2.1 on this report above.

3. NATIONAL SECURITY AND EMERGENCY POWERS

3.1 Electronic Communications Act 2003 (2003:389) (lag (2003:389) om elektronisk kommunikation) (the "ECA")

Under chapter 7, section 8 if a network operator or service provider does not fulfil its obligations under the ECA, and such breach severely threatens the public order, national security or public health or could otherwise be deemed to cause severe economic or operational problems for a supplier or user of an electronic communication network or service, the Swedish Post and Telecommunication Authority (the "PTA") may, with immediate effect, order an injunction against the relevant network operator or service provider.

A PTA decision of this nature is valid for a maximum of three months. If no corrective measures are taken by the network operator or service provider in breach, the period may be extended by a further three months.

The PTA may also revoke a network operator's or service provider's authorisation to use a certain radio transmitter or to use radio transmitters within certain radio frequencies in its business. The PTA may further change the terms and conditions of such authorisations.

In accordance with chapter 1, section 8, if Sweden is (or has recently been) at war or under the threat of war, or if there are extraordinary conditions that are caused by a war outside of Sweden, the government may issue regulations governing electronic communications networks and associated facilities and services, and other radio usage as necessary for the purposes of national defence or security in general. This may result in additional emergency powers for the relevant authorities.

3.2 Proposed Swedish Government Official Report (SOU 2013:33 – en myndighet för alarmering) (the "Report")

The Report provides that certain government agencies will be able to send text messages alerting citizens to emergency situations. The Report defines which government agencies hold this right and who is responsible for the costs that exercising this right entails.

3.3 Further legislative discussion

There have been theoretical discussions held that indicate that the government, under exceptional circumstances (for instance severe threats against national security), would have the right to invoke a constitutional privilege of self-defence (konstitutionell nödrätt) which may entail a wider scope of governmental power than otherwise described in this report. In accordance with page 95 of the preparatory works (SOU 2003:32 – Vår beredskap efter den 11 september: betänkande), the right to act in emergency situations is covered by Chapter 1-12 of the Swedish Form of Government (Regeringsformen (1974:152)), where Parliament's functions are delegated to the government. In situations where delegation powers under the aforementioned chapters do not exist, one option is to act through the constitutional privilege of self-defence.

The constitutional privilege of self-defence has never been exercised, thus making it difficult to properly assess its scope in this context. It is however not unlikely that the government may take control of a network operator's or service provider's network if this is necessary to uphold national security.

4. CENSORSHIP

4.1 Freedom of Press Regulation (tryckfrihetsförordning (1949:105)) and the Freedom of Speech Constitution (yttrandefrihetsgrundlag (1991:1469))

Under the Freedom of Press Regulation and the Freedom of Speech Constitution, there is a prohibition against censorship. The right to express an opinion, without it being censored, is thus a constitutional right in Sweden.

4.2 Code (1942:740) of Judicial Procedure (Rättegångsbalk (1942:740) (the "CJP")

As described above, under chapter 27, section 19, data may be secretly intercepted via real-time interception of electronic communications.

Government agencies have the right to prevent the customer communications (described above) from reaching its recipient where there is an on-going investigation relating to the discovery of offences which may include hacking, child pornography and drug crimes.

Government agencies also have the right to switch off a phone number in critical situations to prevent a suspect from contacting his or her accomplices or receiving warning calls.

4.3 Electronic Communications Act 2003 (2003:389) (lag (2003:389) om elektronisk kommunikation) (the "ECA")

Under chapter 7, section 9a, the Consumer Ombudsman (Konsumentombudsmannen) may order a network operator or service provider to prevent user access to a number whose digit structure lacks a geographical sense, if the marketing of the number or the service related to it is improper or if material information is omitted in the marketing material. This means that it may become impossible for users to reach the number or service in question.

Certain Internet Service Providers have entered into voluntary cooperation agreements with the Police Authority to block DNS that contain child pornography material. The content and scope of such agreements are confidential.

Moreover, in a recent judgement delivered by the Swedish Patent and Market Court of Appeal on February 13 2017, the court declared that an internet service provider that acts as an intermediary can be ordered to block access to websites that infringe intellectual property rights. As a consequence, the court issued an injunction, combined with a conditional fine, that required the internet service provider Bredbandsbolaget (Telenor) to block subscribers from accessing illegal streaming and piracy websites, The Pirate Bay and Swefilmer.

4.4 Other legislation on obligation to disclose subscriber data

The Tax Agency has far reaching powers which enable it to request information from network operators on the use of electronic communications of tax subjects (cf. what is set out above under paragraph 2.1). For example, the Tax Agency may use general tax legislation such as the Law on Taxation Procedures (2011:1244) (skatteförfarandelag (2011:1244)) to request information on subscribers and their use of electronic communications. Such order can be combined with a conditional fine amounting to several million SEK. There are no court approvals prior to the Tax Agency making its decision regarding the obligation to disclose subscriber data upon a conditional fine. However, if the network operators abstains from or objects to complying with the obligation, the obligation will be subject to a court proceeding.

Professional sellers or lessors active in the retail business are by law obliged to disclose information on the purchase of equipment that allows for reception of TV services to Radiotjänst i Kiruna AB. The professional sellers or lessors shall provide Radiotjänst i Kiruna AB with such information about the subscriber that is necessary in order for them to determine the appropriate TV license fee.

According to the Copyright Act (1960:729) (lag (1960:729) om upphovsrätt till litterära och konstnärliga verk) a rights holder can apply for an injunction, subject to a conditional fine, requesting an electronic communications service provider to disclose information regarding the origin and distribution network (i.e. the name and IP address) of the suspected.

5. OVERSIGHT OF THE USE OF POWERS

5.1 Judicial Oversight

Where court approval is provided for an interception or the collection of information pursuant to chapter 27, section 21 CJP, the competent court and the relevant public prosecutor have a supervisory role in the use of the measures that are used.

5.2 The Swedish Post and Telecommunication Authority (Post- och telestyrelsen) (the "PTA")

The PTA generally supervises network operators' and service providers' compliance with their respective obligations. According to chapter 7 of the ECA, the PTA is entitled to order a network operator or service provider to disclose information and documentation needed in order to ensure that the network operator or service provider complies with its obligations. Such order may be combined with a conditional fine. The PTA is also entitled to gain access to any facilities (excluding residences) where a network operator or service provider's business is conducted in order to perform an audit of the business in question.

If the PTA deems that a network operator or service provider has breached its obligations, it may order the network operator or service provider to rectify its breach. Such order may be combined with a conditional fine.

5.3 Inspection of Defence Intelligence (the "IDI")

The IDI supervises the secret defence intelligence activities performed by the National Defence Radio Establishment (the "NDRE"). It may do this, for example, by only permitting the NDRE to intercept signals transmitted in cables which are covered by a court order from the Defence Intelligence Court (Försvarsunderrättelsedomstolen).

5.4 Commission on Security and Integrity Protection (Säkerhets- och integritetsskyddsnämnden) (the "SIN")

All decisions on the collection of data under the Act on Collection of Data in Electronic Communication in the crime combatting Authorities Intelligence Services ("IEUK") shall be communicated to SIN, which supervises the relevant government agencies' compliance with the IEUK.

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

Restrictions on network operators and service providers

6.1 Publicity and Secrecy Act (offentlighets- och sekretesslagen (2009:400)) (the "PSA")

Under the PSA, the government has the legal authority to prevent a network operator or service provider from publishing aggregate data relating to intercept requests or acquisitions of metadata when, for example, secrecy under a current investigation applies to the aggregate data and any publication of the information may jeopardise or impair the investigation. Confidentiality will apply to activities such as those which aim to prevent, detect, investigate or prosecute crime, conducted by prosecutors, the police and the Swedish Security Service.

Neither the public prosecutor nor the Police Authority need to obtain any authority or court order before the information is to be considered confidential.

Confidentiality may also apply to data relating to preliminary investigations in criminal cases or a matter relating to the use of coercive measures, if the purpose of the measures is undermined by disclosure, or if future operations may be damaged by disclosure.

The government does not have the legal authority to prevent a network operator or service provider from publishing descriptions of, or information relating to, the laws described in this report.

Aggregate data published by government agencies.

The Public Prosecution Authority annually publishes a report of the use of secret surveillance-related laws. The report for 2015 is available at: https://www.aklagare.se/globalassets/dokument/rapporter/ovriga-rapporter/redovisning-av-anvandningen-av-vissa-hemliga-tvangsmedel-under-2015.pdf. The report does not include the details of any interception or surveillance initiated by the secret police.

7. CYBERSECURITY

7.1 Electronic Communications Act (2003:389) (Sw. Lag om elektronisk kommunikation) ("the ECA") and the Personal Data Act (1998:204) (Sw. Personuppgiftslagen) ("the PDA")

Under chapter 5, section 6A ECA (which implements the EU legislative package on electronic communications, e.g. Directive 2009/136/EC and Directive 2009/140/EC), a telecommunications network operator or service provider must take appropriate technical and organisational measures (including cybersecurity measures) to appropriately manage any risks posed to the security of networks and services. In particular, such measures have to provide safeguards to prevent and minimise the impact of security incidents on users and interconnected networks.

In the context of personal data protection, the ECA and PDA, which implement Directive 95/46/EC and contain regulations pertaining to cybersecurity in the context of personal data processing, stipulate that a data controller or processor (e.g. a telecommunications service provider) has to take appropriate cybersecurity measures to protect personal data. These measures must provide for an appropriate level of security based on (i) the technical possibilities available; (ii) the costs of the intended measures; (iii) the specific risks linked to the processing of the personal data; and (iv) the sensitivity of the personal data.

Pursuant to the ECA and the PDA, the regulator can use several supervisory measures to ensure compliance with the legislation (which includes requirements related to the protection against cybersecurity). In summary, the PTA:

(a) is entitled to receive any information and documentation required to conduct its supervision and can require access to the premises and infrastructure of the telecommunications operator, including any premises where personal data is processed; and

(b) has the power to issue injunctions and prohibitions to ensure compliance with the legislation and regulations issued pursuant to an Act (for example the PTA Regulation on Information Security (PTSFS 2012:4) (Sw. Post och Telestyrelsens Föreskrifter om krav på driftsäkerhet).

Note however that under current Swedish legislation, there is no general incident reporting obligation owed to the regulator (for example if a service company's database is hacked). Despite this, certain sector-specific regulation pertaining to data breaches in the telecommunications sector should be noted.

One such example is the specific breach notification regime for registered telecommunications operators, as set out in the Commission Regulation (611/2013) and PTSFS 2012:1, This requires that any such notification of a personal data breach by a registered operator is addressed to (i) the regulator and (ii) the individual (or "subscriber") unless the data has been securely encrypted and rendered unintelligible to any person who is not authorised to access it.

The information to be included in the notification to the regulator and the individual affected is specified in the annex to the Commission Regulation and includes:

(a) the service provider's identity and relevant contact details;

(b) the timing and circumstances of the breach;

(c) the nature and content of the data;

(d) the remedies contemplated;

(e) the likely consequences of the breach; and

(f) the technical or organisational measures taken to address the breach.

It is important to note that a notification addressed to the regulator may become publicly available, at least in part, under the Swedish Public Access to Information and Secrecy Act (2009:400) (Offentlighets- och sekretesslagen).

A further example is chapter 5 section 6C ECA which provides that a network operator or service provider must notify the regulator of any IT security breach that has had a significant impact on the operation of their networks or services (for example an attack that has led to a complete shutdown of the operator's critical systems).

It should also be noted that the Swedish legislator is currently in the process of implementing Directive 2016/1148/EU (the "NIS Directive"). This NIS Directive aims to ensure a high common level of network and information security across the EU but does not extend to public telecommunication service providers. Note however, that it is not yet clear how the Swedish legislator will implement the NIS Directive. Accordingly, this information should (for the time being) be treated with caution until the NIS Directive has been fully implemented.

The forthcoming General Data Protection Regulation 2016/679/EU (the "GDPR"), which enters into force in 2018 will define the requirements with regard to cybersecurity for personal data and will further require data controllers and data processors to implement a general personal data breach notification regime (which will include keeping a register of any data breaches).

The Swedish Post and Telecom Authority (Sw. Post och Telestyrelsen) ("the PTA") is the supervisory authority responsible for the administration of the ECA and the PDA in the telecommunications sector. The Swedish Data Protection Authority (Sw. Datainspektionen) ("the DIA") may also supervise compliance with the PDA in cases where personal data processing falls outside of the scope of providing network and telecommunication services.

As referred to above, under chapter 1 section 8 ECA, if Sweden is (or has recently been) at war or under the threat of war, or if there are extraordinary conditions that are caused by a war outside of Sweden, the government holds the right to issue new regulations governing electronic communications networks and any associated facilities and services necessary to providing national defence or security. This may result in additional emergency powers for the regulator and consequently, limitations on the rights of Swedish individuals in regards to their right to property, privacy, a fair trial and freedom of expression.

Chapter 7 section 8 ECA stipulates that if a network operator or service provider does not fulfil its obligations under the law (e.g. their cybersecurity requirements) and this breach severely threatens public order, national security or public health or could otherwise be deemed to cause severe financial or operational problems for the supplier or the users of the electronic communication networks or services, the regulator may, with immediate effect, order an injunction against the relevant network operator or service provider (which effectively acts as a conditional cease operations order).

Note that under the ECA and the PDA, the regulator can in fact combine such injunctions with a conditional fine. Moreover, under the PDA a data controller is liable to pay damages to a data subject for any damage and violation of their personal privacy caused by the processing of personal data in contravention of the PDA, for example by not implementing sufficient cybersecurity measures.

An individual can also be subject to a fine or imprisonment of up to two years, in addition to being liable to pay damages, if he or she intentionally or by gross negligence, processes personal data in contravention of the provisions of the PDA. In practice, the courts more usually impose penalties in the form of fines and damages with custodial sentences being rare. The few custodial sentences that have been handed down by the Swedish courts have generally been in cases involving further offences, such as defamation.

The decisions of the PTA and the DIA can be appealed in the first instance to the Stockholm County Administrative Court (the "County Court"). To appeal a decision of the County Court, leave to appeal must be obtained which then permits the Stockholm Administrative Court of Appeal and if necessary the Supreme Administrative Court, to retry the case.

8. CYBERCRIME

8.1 The Penal Code (1962:700) (Sw. Brottsbalken) (the "PC")

The following acts of cybercrime are punishable under Swedish law:

SECTION	Offence	Penalty
Chapter 4 section 9c,	Illegal access, also referred to 'intrusion' or 'hacking' Defined as "intentionally, and without permission, accessing information aimed to be processed through an automated process". It also includes the illicit alteration, deletion, insertion, blocking or disruption of such data (including Denial of Service Attacks). This cybercrime further includes situations where a perpetrator may be able to illicitly gain access to information (even if he or she did in fact not do so). Note that the term "illegal access" encompasses all forms of data that can be processed by a computer, and includes data permanently stored on a computer (e.g. on a hard drive), temporarily stored for processing (e.g. ones and zeros in the random access memory of a computer) or actual programs processing the previously mentioned forms of data. In this context, it should also be noted that interception of a message conveyed by a telecommunications company may be categorised as the separate offence "illicit access" under chapter 4 sections 8-9 PC.	Fines or imprisonment for up to two years. In cases of gross illegal access (for example in aggravating circumstances such as when material damages have been caused) the penalty is imprisonment for a minimum of six months and a maximum of six years.
Chapter 9 section 2 PC	Computer-related fraud Defined as the act of providing inaccurate or incomplete information by altering a computer program or recording, or otherwise illicitly affecting the outcome of an automated information process or a similar automated process, so that the offender benefits to the detriment of someone else. This provision therefore encompasses computer system or data manipulation which is carried out for financial profit i.e. the copying of magnetic strips on credit cards ('skimming') and 'phishing' attacks where, for example, copies of banks' web pages would be set up in order to steal the bank's customers' login details.	Fines or imprisonment for up to six months. Under aggravating circumstances the offender may be sentenced to imprisonment for a minimum of six months and a maximum of six years.

Additionally, if any of the criminal acts described above cause loss, this may lead to criminal liability for damages.

The authorities responsible for the administration of cybercrime legislation are the Swedish Ministry of Justice and the National Police Authority.

Chapter 2 section 4 PC stipulates that the legislation on cybercrime has extraterritorial reach, provided that the criminal act in question is directed towards Swedish data or Swedish IT-systems (e.g. non-nationals engaged in hacking activities in the jurisdiction).

Criminal cases pertaining to cybercrime are adjudicated by the general courts, i.e. the district courts, the Court of Appeal and the Supreme Court. If an offender has been sentenced to a fine in the district court and wishes to appeal this, a leave of appeal is necessary. Leave of appeal is also necessary should an appeal to the Supreme Court be sought by a defendant.

Law stated as at 17 February 2017.

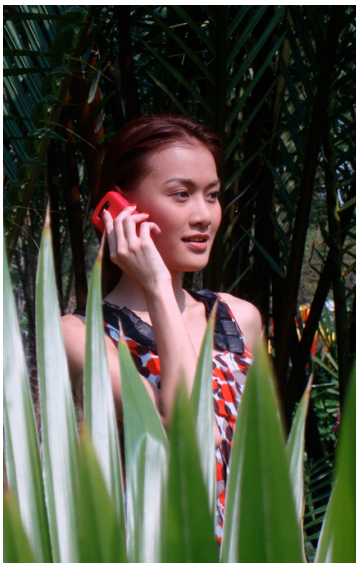
THAILAND – COUNTRY REPORT

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.