ASSESSING CYBERCRIME LAWS FROM A HUMAN RIGHTS PERSPECTIVE

GLOBAL PARTNERS DIGITAL

The development of this document was made possible with support from the United States Department of State.

GPD is grateful to all those who provided comments and feedback on earlier drafts of the document.

Contents

Foreword

This tool aims to support the development of human rights-respecting cybercrime legislation. Drawing upon international standards, it provides a standalone framework for assessing the different elements of cybercrime legislation from a human rights perspective. It also provides examples of good and poor practice from existing pieces of cybercrime legislation across the world, and highlights further considerations, beyond the text of the legislation, that governments and other stakeholders should take into account when developing or revising cybercrime legislation.

HOW DO I USE THE GUIDE?

Section 1 of this tool sets out a brief background of cybercrime as an issue, what cybercrime legislation looks like, and how to use this tool. Section 2 provides a framework for analysing the key elements of cybercrime legislation, how these can respect and protect human rights, and provides examples of good practice seen in existing cybercrime legislation. Section 3 sets out further considerations, beyond the text of the legislation itself, that are necessary when it comes to enforcement.

Annex 1 to this tool provides definitions of some of the key terms used in this tool (these are all highlighted in bold blue text throughout the tool), while Annex 2 distils the tool into a summary of 10 key things to look out for in cybercrime legislation from a human rights perspective. Annex 3 sets out a list of real life examples—both good and bad—of cybercrime legislation.

WHO IS THIS GUIDE FOR?

The tool can be used both by those within governments who are developing or revising legislation themselves and other stakeholders, such as civil society organisations, who are engaging in that process.

While designed primarily for use at the point at which cybercrime legislation is being developed or revised, it can also be used to assess existing cybercrime legislation to identify areas where reform might be needed.

METHODOLOGY

The methodology used in this tool is based on international human rights law, primarily the International Covenant on Civil and Political Rights (ICCPR) as well as its elaboration and interpretation by UN Treaty Bodies. It also substantially draws on the Council of Europe's Convention on Cybercrime (the Budapest Convention), which came into force in 2004 as the first multilateral treaty on cybercrime. For a more detailed rationale for our methodological approach, see Annex 4.

01

Understanding cybercrime legislation

In this section, we first set out an explanation of what cybercrime is and what cybercrime legislation looks like. We then explain how to use this tool to assess specific elements of cybercrime legislation from a human rights perspective.

What is cybercrime?

While there is no single, universally used definition of "cybercrime", criminal offences which can constitute cybercrimes can be divided into two broad categories:

1. Cyber-dependent crimes: crimes that can be committed only through the use of computers and other ICTs. e.g unauthorised data access and interference (or, hacking).
2. Cyber-enabled crimes: crimes which can be committed without computers or ICTs, but can also be committed, and potentially increased in scale or reach, with them. e.g. fraud

In practice, the line between these two categories is sometimes blurred and cybercrime legislation may not make a distinction between them.

While cyber-dependent crimes, because of their nature, require specific criminal offences which make reference to the use of ICTs, the same is not necessarily true for cyber-enabled crimes. A criminal offence of fraud or theft, for example, can be committed either using ICTs or without them.

In the majority of cases, a generally worded criminal offence should be able to cover both categories of cybercrime. In some cases, depending on the nature of the criminal offence, all that might be needed is to ensure that the wording of the offence explicitly includes language that ensures that it would apply to situations where it is committed using ICTs.

What is cybercrime legislation?

Cybercrime legislation will ordinarily comprise two types of provisions:

1. Substantive elements: the specific criminal offences that are prohibited.
2. Procedural elements: the tools, mechanisms and powers established by the legislation to facilitate the investigation and prosecution of those criminal offences.

Depending on the particular legal system in a state, cybercrime legislation can take different forms. It might be a standalone piece of legislation, spread across different pieces of legislation, or part of a much more comprehensive instrument, such as a Criminal or Penal Code.

As explained in the Methodology in Annex 4, this tool draws in particular upon the Budapest Convention, in relation to both substantive and procedural elements. From a human rights perspective, the Budapest Convention—while not perfect—is the best existing example of a framework which, if incorporated appropriately into domestic legislation, mitigates risks to human rights, and actively protects and enhances the enjoyment of human rights.

02

Framework for analysing cybercrime legislation

This section looks at different elements of cybercrime legislation. For each element, we set out what its links are to human rights, what a rights-respecting provision should look like, and any further considerations that you should bear in mind when developing or reviewing the element. A list of good (and bad) examples for each of the elements covered can be found in Annex 3.

Substantive elements

Cyber dependent crimes

(i) Unauthorised access

Why is this important from a human rights perspective?

Criminal offences of unauthorised access help protect individuals' right to privacy, both by ensuring that they alone have control over their property (which includes their computers and devices) and the information, communications or data contained within.

How should this element be formulated in the law?

- The criminal offence should prohibit the access to a computer system, or any part of one, without authorisation.
- The criminal offence should require an intention to access the computer system, or any part of one, and knowledge that it is unauthorised.

What further considerations are needed?

- Some states require additional elements to be satisfied for the offence to be committed, e.g. that it involves the infringement of security measures, is done with the intent of obtaining computer data or some other dishonest intent, or is done in relation to a computer system that is connected to another computer system. But a broader offence without these qualifications is preferable from a human rights perspective, as it captures more activity that could potentially infringe upon the right to privacy.
- Some model laws include further criminal offences, like "unauthorised remaining" (remaining logged into a computer system, or continuing to use it) and "data espionage" (obtaining computer data which are not meant for the person). Such offences are unnecessary.

(ii) Unauthorised interception

Why is this important from a human rights perspective?

The purpose of prohibiting unauthorised interception of the transmission of data is to prevent people from being able to access or view others' information, data or communications where they are not authorised to do so. This has strong links to the right to privacy, since it relates to individuals' control over their information, communications and data.

How should this element be formulated in the law?

The criminal offence should prohibit the unauthorised interception by technical means of either any non-public transmission to, from or within a computer system; or electromagnetic emissions from a computer system that are carrying computer data.

The criminal offence should require an intention to intercept the transmission or emissions.

What further considerations are needed?

Some states require additional elements to be satisfied for the offence to be committed, e.g. that there be dishonest intent, or that the interception take place in relation to a computer system that is connected to another computer system. As above, a broader offence without these qualifications is preferable from a human rights perspective.

(iii) Data interference

Why is this important from a human rights perspective?

Criminal offences of data interference can therefore protect individuals' right to privacy by ensuring that they retain control over the information, communications or data contained within their computers and other devices.

How should this element be formulated in the law?

- The criminal offence should prohibit the damaging, deletion, deterioration, alteration or suppression of computer data without authorisation.
- The criminal offence should require an intention to commit one of these acts.

What further considerations are needed there?

- It might be beneficial to clarify that an offence can be committed regardless of whether the effect of the act is permanent or temporary.
- Some states require additional elements to be satisfied for the offence to be committed, e.g. that the act resulted in serious harm. While the Budapest Convention allows countries to make their own interpretations of what constitutes such serious harm, its Explanatory Report provides that "Parties should notify the Secretary General of the Council of Europe of their interpretation if use is made of this reservation possibility".

(iv) System interference

Why is this important from a human rights perspective?

Criminal offences of system interference help protect individuals' right to privacy by ensuring that they alone have control over the data contained within their computers and other devices, and protect their right to freedom of expression by ensuring that communications remain open and uninterrupted.

How should this element be formulated in the law?

- The criminal offence should prohibit hindering or interfering with the functioning of a computer system, or with a person who is lawfully using or operating a computer system, without authorisation.
- The criminal offence should require an intention to commit one of the acts.

What further considerations are needed there?

- It might be beneficial, for the purpose of legal certainty, to clarify that "hinder" includes (but is not limited to):
- cutting the electricity supply to a computer system;
- causing electromagnetic interference to a computer system;
- corrupting a computer system by any means; and
- inputting, destroying, deleting or altering computer data.

Some model laws include a further offence of interfering with systems used for critical infrastructure operations. The Budapest Convention does not make this distinction—which is best practice, as it avoids both the duplication of offences, and potential risks arising from an overly broad definition of "critical infrastructure".

(v) Offences relating to the misuse of items

Why is this important from a human rights perspective?

As cyber-dependent crimes, committing one of the four offences listed above necessitates the use of a computer, and potentially other "items" (the term used in the Budapest Convention), such as pieces of physical equipment, computer programs, or passwords. These items are often developed specifically to be used to commit cyber-dependent crimes (and, potentially, cyber-enabled crimes).

Creating offences relating to these items—such as their production, sale or supply— can help further reduce the occurrence of cybercrimes by making it less likely that the necessary items will be accessible to those who wish to commit them. They therefore indirectly help protect individuals' rights to privacy and freedom of expression.

How should this element be formulated in the law?

The criminal offence should prohibit the following acts, without authorisation:

- producing, selling, procuring for use, importing, exporting, distributing or otherwise making available:
- a device, including a computer program, that is designed or adapted for the purpose of committing one of the four offences listed above; or
- a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed; or
- having an item mentioned above in his or her possession.

The criminal offence should require an intention that the item be used by the person, or any other person, for the purpose of committing one of the four cyber-dependent offences listed above.

Substantive elements

Cyber enabled crimes

(i) Computer-related forgery

Why is this important from a human rights perspective?

Unlike almost all other cybercrimes listed in this tool, offences of forgery do not have any particular impact upon the rights to privacy or freedom of expression. They can, of course, still lead to other societal and individual harms.

How should this element be formulated in the law?

- The criminal offence should prohibit the unauthorised input, alteration, deletion, or suppression of computer data, resulting in inauthentic data.
- The criminal offence should require an intention that the computer data be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible.

What further considerations are needed there?

Some states have taken a narrower approach to the mental culpability requirement of this criminal offence and require an additional qualifying element, such as an intention to defraud, or for there to be some other dishonest intent.

(ii) Computer-related fraud

Why is this important from a human rights perspective?

Computer-related fraud is included in the Budapest Convention to reflect the fact that many assets are now represented in computer systems. Offences of fraud can adversely impact upon the right to privacy, primarily when an individual fraudulently impersonates another or assumes their identity.

How should this element be formulated in the law?

- The criminal offence should prohibit the unauthorised causing of a loss of property to another person through the input, alteration, deletion or suppression of computer data, or an interference with the functioning of a computer system.
- The criminal offence should require an intention to fraudulently or dishonestly procure an economic benefit for oneself or another person.

(iii) Offences related to child sexual abuse material

Why is this important from a human rights perspective?

The ability to create and distribute images and videos online has made it far easier for images and videos of child sexual abuse (child sexual abuse material) to be shared. While not primarily considered as infringing the rights to privacy or freedom of expression, the sexual abuse of children is a gross violation of children's rights.

How should this element be formulated in the law?

The criminal offence should prohibit the following:

- producing child sexual abuse material for the purpose of its distribution through a computer system;
- offering or making available child sexual abuse material through a computer system;
- distributing or transmitting child sexual abuse material through a computer system;
- procuring child sexual abuse material through a computer system for oneself or for another person;
- possessing child sexual abuse material in a computer system or on a computer-data storage medium.

The offence should require an intention to commit any of the above acts.

What further considerations are needed there?

It might be beneficial to clarify that there are certain, limited defences when the person's actions were for a legitimate scientific, research, media or law enforcement purpose.

(iv) Other substantive offences

As noted above, there is not always a need for cyber-enabled crimes to be addressed through specific criminal offences which only apply when their commission involves ICTs.

However, there are various examples of cybercrime legislation which include additional substantive offences. Some of these, such as provisions prohibiting the non-consensual sharing of intimate images, may be considered rights-promoting provisions. But many of these offences, including those provided below, are broadly worded and pose risks to human rights, particularly freedom of expression. We present a few examples of bad practice in Annex 3.

Procedural elements

(i) Expedited preservation of computer data

Why is this important from a human rights perspective?

This relates to the preservation of computer data held by telecommunications or internet service providers, so that it can be used by law enforcement in their investigations. This data may well include personal information, however, and therefore falls within the scope of concerned individuals' rights to privacy.

How should this element be formulated in the law?

- The provision should require that any order to preserve computer data be made by an individual of at least a specified rank within a competent authority, such as a police officer.
- The provision should only enable the individual to order or obtain the computer data in specified criminal investigations or proceedings, and not generally.
- The provision should require the individual to be satisfied that the computer data that is the subject of the order is "reasonably required for the purposes of a criminal investigation".
- The provision should also require the individual to be satisfied that "there is a risk that the computer data may be destroyed or rendered inaccessible".
- The provision should require that any order be made by written notice to the person who is in control of the computer system.
- The provision should set a maximum period for which the computer data must be preserved.
- The provision should not require a service provider to collect or retain any particular data, nor should the provision require them to introduce new technical capabilities. Nor should the provision enable the automatic disclosure of the data to the competent authority. Data disclosure should be regulated under a separate provision (see below, under "Production orders").
- The provision should ensure that any order to preserve traffic data can be made to multiple service providers where more than one was involved in the transmission of that traffic data.

(ii) Production orders

Why is this important from a human rights perspective?

Since computer data and subscriber information—often crucial to law enforcement investigations—is generally held by third parties, cybercrime legislation usually includes provisions to enable the law enforcement to gain access to it. As both computer data and subscriber information include personal information, this provision can pose risks to individuals' rights to privacy.

How should this element be formulated in the law?

- The provision should require that any order to produce computer data or subscriber information should be made by a judge or magistrate.
- The provision should require that any application for a production order be made by an individual of at least a specified rank within a competent authority, such as a police officer.
- The provision should only enable a production order to be made in relation to specified computer data or subscriber information.
- The provision should only enable a production order to be made for the purposes of specified criminal investigations or proceedings, and not generally.

- Where a production order for computer data which constitutes content data is being sought, the provision should only enable this to be made for the most serious offences which should themselves be enumerated in the legislation.
- The provision should require the judge or magistrate to be satisfied that the computer data or subscriber information that is the subject of the order is "reasonably required for the purpose of a criminal investigation or criminal proceedings".
- For computer data, it should only be possible for a production order to be directed toward a person where that data is under the person's "possession or control".
- For subscriber information, it should only be possible for a production order to be directed toward the relevant service provider.
- The provision should not require a person or a service provider to collect or retain any particular data or information, nor should the provision require them to introduce new technical capabilities.

(iii) Search and seizure of computer data

Why is this important from a human rights perspective?

Powers for law enforcement agencies to seize and search physical items for the purpose of criminal investigations and proceedings are a standard part of criminal procedural law. In some jurisdictions, these general powers may also be available in relation to computer data, in which case separate provisions may not be needed. However, in many jurisdictions, these general powers do not apply, or sit awkwardly with the non-physical nature of computer data, making specific powers necessary. As with the seizure and search of any physical items, the right to privacy is almost always engaged by the search and seizure of computer data, which is likely to contain personal information.

How should this element be formulated in the law?

There is rarely one standard procedural provision for this. Sometimes it will be proportionate for a law enforcement agent to be able to seize and search items when a person is arrested—e.g. if an item in their possession obviously relates to that offence. In other situations, proportionality may require a warrant or order from a magistrate or judge beforehand.

(iv) Real-time collection of traffic data

Why is this important from a human rights perspective?

Being able to access and collect traffic data in real time, in appropriate circumstances, is critical to ensuring that law enforcement agencies are able to investigate and prevent cybercrimes before harm is caused, or to mitigate their impact. However, the interception of traffic data is an intrusion into affected individuals' right to privacy; revealing who they are communicating with, when and for how long, their location at the time of the communications, as well as the websites that they visit.

How should this element be formulated in the law?

- The provision should allow competent authorities to access or collect traffic data - with the assistance of service providers if necessary - in real time, if certain conditions (set out below) are met.
- The provision should also allow competent authorities to require service providers to collect traffic data in real time, and to provide it to those authorities, if certain conditions (set out below) are met.
- The provision should require that any traffic data collected or recorded can only be accessed by a competent authority with judicial authorisation, or an individual of at least a specified rank within the competent authority.
- The provision should only enable the collection or recording of traffic data in relation to specified communications and for a specified duration, rather than generally.
- The provision should require the authorising judge or individual of at least a specified rank to be satisfied that access to the traffic data is relevant to a particular criminal investigation and a proportionate measure.

(v) Interception of content data

Why is this important from a human rights perspective?

- Content data refers to the content of a communication, i.e. the actual message or information being conveyed by a communication, as opposed to the traffic data. This content data can be criminal in and of itself—e.gif it is child pornography—or evidence of another criminal offence, such as communications which reveal the planning of a crime.
- However, the interception of content data is a heavy intrusion into affected individuals' right to privacy, meaning that strong safeguards are necessary to ensure that the power is only available when necessary and proportionate.

How should this element be formulated in the law?

- The provision should allow competent authorities to access or collect content data - with the assistance of service providers if necessary - in real time, if certain conditions (set out below) are met.
- The provision should also allow competent authorities to require service providers to collect content data in real time, and to provide it to those authorities, if certain conditions (set out below) are met.
- The provision should require that any content data recorded can only be accessed by a competent authority with judicial authorisation, or an individual of at least a specified rank within the competent authority.
- The provision should only enable access to content data in relation to specified content data or a specified individual, and for a specified duration, rather than generally.
- The provision should only enable access to content data in relation to the most serious offences and these should be set out in law.
- The provision should require the authorising judge or individual of at least a specified rank to be satisfied that access to the content data is necessary and proportionate, and that no less intrusive measure would be effective in achieving the aim sought.

03

Conditions and safeguards

As noted in Section 1, states have obligations under international human rights law to respect, protect and promote human rights. In this Section, we outline how cybercrime legislation can align with these obligations.

Conditions and safeguards

Cybercrime legislation needs to be drafted, implemented and enforced in a way consistent with states' obligations under international human rights law.

Recognition of this requirement is reinforced in the Budapest Convention which, through Article 15, requires states parties to:

"ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality."

There are a number of levels at which conditions and safeguards can exist:

- In relation to each specific criminal offence or procedural provision;
- In relation to cybercrimes generally;
- In relation to the criminal law generally; and
- In relation to the national legal framework generally.

The necessary conditions and safeguards for each specific criminal offence or procedural provisions are set out in Section 3 of this guide. However, states should also consider what further conditions and safeguards are necessary in relation to the three other levels. While this section of the guide does not provide a comprehensive list of those conditions and safeguards, there are a number which will be common across states and should be considered essential.

Conditions and safeguards in relation to cybercrimes generally

The procedural provisions which give powers to law enforcement agencies should only be used in relation to the specified cybercrimes.
There should always be a requirement that clearly articulated thresholds are met before a judge or magistrate is able to authorise certain actions.
There should always be a requirement for any action taken to be proportionate, and for the rights of individuals and third parties to be taken into account.

Conditions and safeguards in relation to the criminal law generally

There should be sufficient training for judges and law enforcement agencies on cybercrime legislation and human rights, as part of their broader training.
There should be effective and independent oversight of the actions of law enforcement agencies and the use of their powers under cybercrime legislation.
The criminal law should ensure general procedural rights, including the presumption of innocence, the

right to fair trial, equality of arms, and the prohibition of prosecution for the same offence more than once.
The criminal law should allow for appropriate defences to criminal offences, such as necessity and duress.
The criminal procedural law should allow for prosecutorial discretion not to prosecute offences where it would not be in the public interest to do so.

Conditions and safeguards in relation to the national legal framework generally

The existence of a fully independent and impartial judicial system, and respect for the rule of law.
The existence of a general human rights framework in the state - either through the constitution or specific legislation - which obliges public authorities, including law enforcement agencies, to act compatibly with human rights, and through which legislation and the actions of public authorities can be challenged on human rights grounds.

Annexes

Annex 1: Terminology

Access: The term "access" is not defined in any existing frameworks, however the Explanatory Report to the Budapest Convention notes that it should include "the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data)" but that it would not include "the mere sending of an e-mail message or file to that system".

Authorisation: The term "authorisation" means either the express permission of the owner of the computer or device, or some other lawful reason or justification. See also "unauthorised".

Child sexual abuse imagery / child pornography: While the term "child pornography" is increasingly seen as inappropriate given that it suggests a degree of complicity or consent on the part of the child, it is still the term used in many legal instruments, including the Budapest Convention. The term "child sexual abuse material" (CSAM) (or sometimes "child sexual abuse imagery" (CSAI)) is now considered to be more appropriate to describe the phenomenon.

The term is partially defined in the Budapest Convention as including "pornographic material that visually depicts: (a) a minor engaged in sexually explicit conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; or (c) realistic images representing a minor engaged in sexually explicit conduct".

- Note 1: The Budapest Convention leaves it to the discretion of states parties as to what age a person should be considered "minor", suggesting that it include all persons under the age of 18 years, but allowing states parties to set a lower age limit of not less than 16 years.
- Note 2: The Budapest Convention allows states parties to exclude (b) and (c) from the definition of "child pornography".

Competent authority: The "competent authority" in a state is the judicial, administrative or other law enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of procedural measures for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings.

Computer data: The term "computer data" is defined in the Budapest Convention as:

"Any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function".

Computer system: The term "computer system" is defined in the Budapest Convention as:

"Any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data".

Content data: The term "content data" is not defined in the Budapest Convention, but should be understood to refer to the content of a communication, i.e. everything that is part of a communication that is not traffic data.

Service provider: The term "service provider" is defined in the Budapest Convention as:

"(a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
(b) any other entity that processes or stores computer data on behalf of such communication service or users of such service."

Specified rank: The term "specified rank" refers to the rank of individual within the state's competent

authority who has sufficient seniority to be able to order, authorise or undertake the execution of procedural measures for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings.

Subscriber information: The term "subscriber information" is defined in the Budapest Convention as:

"Any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

(a) the type of communication service used, the technical provisions taken thereto and the period of service;
(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
(c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement."

Traffic data: The term "traffic data" is defined in the Budapest Convention as:

"Any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."

Unauthorised: An action should be deemed to be unauthorised unless it took place with the express permission of the owner, or the person who took the action had a lawful reason or justification to do so.

Annex 2: Key points to look out for in cybercrime legislation

1. The criminal offence should generally be limited to, and modelled on, those contained in the Budapest Convention.
2. Each criminal offence should be provided for in a stand-alone section or article in national legislation. Even similar offences, such as data interference and system interference, should not be combined but provided as separate offences.
3. The wording of criminal offences and procedural elements should reflect the technically-neutral language used in the Budapest Convention. Technology specific offences or non-neutral terms should be avoided.
4. Any cyber-enabled criminal offences which prohibit certain forms of online content or activity should be clear and precise in scope, pursue a legitimate aim listed under Article 19(3) of the International Covenant on Civil and Political Rights, and be proportionate.
5. Any cyber-enabled criminal offences which prohibit certain forms of online content or activity should be consistent with criminal offences relating to offline forms of expression and activity. Both the scope and potential punishments should be consistent. Forms of expression or activity should not be prohibited solely when they take place online.
6. Any procedural provisions which give law enforcement agencies powers which interfere with the right to privacy should be limited to the most serious criminal offences and time-limited.
7. Any procedural provisions which give law enforcement agencies powers which interfere with the right to privacy should ordinarily require authorisation from a judicial authority. Where this is not possible, and for less intrusive measures only, exercise of the powers should at least require authorisation from an individual within the law enforcement agency with a high level of seniority.
8. Any procedural provisions which give law enforcement agencies powers which interfere with the right to privacy should only be permissible where an assessment has been made their particular use is necessary and proportionate, and then alternative measures would be less effective.
9. Sanctions for criminal offences or non-compliance with procedural powers should be effective, proportionate and dissuasive. Disproportionate penalties, such as excessive fines or periods of imprisonment, should be avoided, and judges given discretion to ensure that they impose an appropriate sanction.
10. The legislation should not authorise internet shutdowns, network disruptions or any other measure which restricts the ability of individuals to use the internet.

Annex 3: Good and bad examples of practice

For each element of a cybercrime law, as set out in the Framework, we've chosen a real life example of good practice, drawn from different countries around the world. The text for each of these good practice examples can be taken as a "model"—insofar as it aligns with the core provisions and parameters of the Budapest Convention. We've also highlighted a few examples of bad practice, and explained why these fall short of a rights-respecting approach.

Substantive elements

Cyber-dependent crimes

(i) Unauthorised access

Good Practice (Botswana): Section 4(1)(a) of the Cybercrime and Computer Related Crimes Act, 2018 prohibits unauthorised access. It provides that "any person who (a) intentionally accesses or attempts to access the whole or any part of a computer or computer system knowing that the access he or she intends to secure is unauthorised (...) commits an offence".

This provision is closely modelled on the wording of the offence of illegal access in the Budapest Convention.

(ii) Unauthorised interception

Good Practice (Tonga): Section 7 of the Computer Crimes Act prohibits "illegal interception of data" and provides that "A person who, willfully without lawful excuse, intercepts by technical means: (a) any transmission to, from or within a computer system; or (b) electromagnetic emissions from a computer system that are carrying computer data, commits an offence".

This provision is closely modelled on the wording of the offence of illegal interception in the Budapest Convention.

(iii) Data interference

Good Practice (Tanzania): Section 7(1) of the Cybercrimes Act 2015 prohibits "illegal data interference" and provides that "A person who intentionally and unlawfully (a) damages or deteriorates computer data; (b) deletes computer data; (c) alters computer data; (d) renders computer data meaningless, useless or ineffective; (e) obstructs, interrupts or interferes with the lawful use of computer data; (f) obstructs, interrupts or interferes with any person in the lawful use of computer data; or (g) denies access to computer data to any person authorized to access it, commits an offence".

This provision contains all the essential elements of the offence of data interference in the Budapest Convention.

(iv) System interference

Good Practice (Romania): Article 45 of the Law 161/2003 on preventing and fighting cybercrime prohibits "system interference". It provides "The act of causing serious hindering, without right, of the functioning of a computer system, by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to such data is a criminal offence".

This provision is closely modelled on the wording of the offence of system interference in the Budapest Convention. While the mental element is not provided for in this particular article, the Criminal Code specifies that intention is required.

(v) Offences relating to the misuse of items

Good Practice (Philippines): Section 4(a)(5) of the Cybercrime Prevention Act of 2012 provides that the following are criminal offences:

"(i) The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:

(aa) A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act; or
(bb) A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act.

(ii) The possession of an item referred to in paragraphs 5(i)(aa) or (bb) above with intent to use said devices for the purpose of committing any of the offenses under this section".

These provisions are closely modelled on the wording of the offence of misuse of devices in the Budapest Convention.

(b) Cyber-enabled crimes

(i) Computer-related forgery

Good Practice (Fiji): Section 9 of the Cybercrime Act 2020 prohibits computer-related forgery and provides that "A person who without lawful authority or reasonable excuse inputs, alters, deletes or suppresses computer data, resulting in inauthentic data with the intention of obtaining a gain for the person or another person, or causing loss to another person or exposing another person to risk of loss, commits an offence".

This provision is closely modelled on the wording of the offence of computer-related forgery in the Budapest Convention.

(ii) Computer-related fraud

Good Practice (Antigua and Barbuda): Section 7(1) of the Electronic Crimes Act 2013 provides that: "A person commits the offence of electronic fraud if that person intentionally and without lawful excuse, induces another person to enter into a relationship with intent to defraud that person or cause that other person to act to his own detriment, or suffer financial loss or loss of property, by – (a) any input, alteration, deletion, or suppression of computer data; or (b) any interference with the functioning of an electronic system".

This provision contains all essential elements of the offence of computer-related fraud in the Budapest Convention.

(iii) Offences related to child sexual abuse material

Good Practice (Nigeria): Section 23 of the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 provides that "(1) Any person who intentionally uses any computer system or network in or for (a) producing child pornography; (b) offering or making available child pornography; (c) distributing or transmitting child pornography; (d) procuring child pornography for oneself or for another person; (e) possessing child pornography in a computer system or on a computer-data storage medium: commits an offence".

This provision is closely modelled on the wording of offences related to child pornography in the Budapest Convention.

Bad Practice (Oman): Article 14 of the Cybercrime Law provides that "The penalty with imprisonment for a period not less than one month and not exceeding one year and a fine not less than OMR one hundred and not exceeding OMR one thousand or by either penalty, shall be applied to any person who uses the informational network or the information technology facilities to produce or procure or distribute or make available or transmit or sale or purchase or import pornography materials, unless such actions were permitted for scientific or technical purposes. The punishment shall be for a period not less than one year and not exceeding three years and a fine not less than OMR one thousand and not exceeding OMR five thousands if the subject matter of the pornography program is a juvenile of less than eighteen years of age or he is meant by the criminal act and the same punishment shall be applied to any person who uses the informational network or the facilities of the information technology to possess juvenile pornography".

This provision criminalises both pornography and child sexual abuse material, which would deviate significantly from the Budapest Convention.

(iv) Other substantive offences

Bad Practice (Cameroon): Section 78 of the Law N° 2010/012 of 21 December 2010 on Cybersecurity and Cybercrime in Cameroon broadly prohibits the dissemination of false information and provides that

"(1) Whoever uses electronic communications or an information system to design, to publish or propagate a piece of information without being able to attest its veracity or prove that the said piece of information was true shall be punished with imprisonment for from 06 (six) months to 02 (two) years or a fine of from 5,000,000 (five million) to 10,000,000 (ten million) CFA francs or both of such fine and imprisonment.

(2) The penalties provided for in Subsection 1 above shall be doubled where the offence is committed with the aim of disturbing public peace."

This provision may pose risks to individuals' right to freedom of expression online because it is unclear how to determine whether information is true, or the scope of what information is covered by this law. Section 78 does not provide clear guidance for individuals and could provide an overly wide degree of discretion to those charged with the enforcement of this law.

Bad Practice (Saudi Arabia): Article 7(1) of the Anti-Cyber Crime Law prohibits "cyber terrorism" and provides that "Any person who commits one of the following cyber crimes shall be subject to imprisonment for a period not exceeding ten years, and a fine not exceeding five million riyals or to either punishment:

(1) The construction or publicising of a website on the information network or on a computer for terrorist organisations to facilitate communication with leaders or members of such organizations, finance them, promote their ideologies, publicise methods of making incendiary devices or explosives, or any other means used in terrorist activities."

While the criminalisation of terrorist content online is not in and of itself a threat to freedom of expression, this particular offence is superfluous as it would not cover activity that is not already prohibited in a general terrorism-related offence. Creating separate offences for activity when they take place with and without a computer is not always appropriate. In most cases, as with this one, a generally worded offence should be able to cover the different ways that it can be committed, including through the use of a computer system.

Bad Practice (Uganda): Section 24(2) of the Computer Misuse Act, 2011 prohibits "cyber harassment" and provides that "For purposes of this section cyber harassment is the use of a computer for any of the following purposes—(a) making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent; (b) threatening to inflict injury or physical harm to the person or property of any person; or (c) knowingly permits any electronic communications device to be used for any of the purposes mentioned in this section."

Section 24(2)(a) poses a clear threat to freedom of expression as it broadly prohibits any requests, suggestions or proposals which are "obscene, lewd, lascivious or indecent". However, section 24(2)(b) which prohibits "threatening to inflict injury or physical harm to the person or property of any person" is likely to be a permissible

restriction as the offence is clear in scope and would pursue a legitimate aim under international human rights law.

Still, as noted above, creating separate offences for activity when they take place with and without ICTs is rarely appropriate. In this case, it would be best practice to instead ensure that the wording of the offline offence explicitly includes language that ensures that it would apply to its commission via computer system, particularly when there are specifics around its commission in those circumstances that do not exist otherwise.
Bad Practice (Kuwait): Article 6 of the Law on Combating Information Technology Crimes prohibits "challenging, ridiculing or insulting God, the Holy Quran, the Prophets, the good companions or the wives of the Prophet, "criticising the Emir or quoting him without a special permission written by the Emiri Diwan" and "insulting the judiciary or members of the Public Prosecution or infringing on the integrity and neutrality of the judiciary or the decisions of the courts or the investigative bodies".

Article 6 of this law imposes sanctions for insulting religion and religious figures, and for criticising the Emir or the judicial system online. These offences pursue aims which are not legitimate and would not constitute permissible restrictions on freedom of expression under international human rights law.

Procedural elements

(a) Expedited preservation of computer data

Good Practice (Nauru): Section 27 of the Cybercrimes Act 2015 regulates the expedited preservation of computer data. It specifies that:

"(1) Where a police officer is satisfied that: (a) electronic data is stored in an electronic device is reasonably required for the purpose of a criminal investigation; and (b) there is a risk that the data may be destroyed or rendered inaccessible, the police officer may, by written notice given to a person in control of the electronic device, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days.

(2) A judge, magistrate or registrar may upon application authorise an extension not exceeding 14 days."

This provision is closely modelled on the procedural provision of 'expedited preservation of stored computer data' in the Budapest Convention. It also contains relevant safeguards and conditions as provided for in Article 15 of the Convention.
(b) Production orders

Good Practice (Mauritius): Section 13 of the Computer Misuse and Cybercrime Act 2003 specifies the procedure for a production order and provides that "(1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigatory authority may apply to the Judge in Chambers for an order compelling – (a) any person to submit specified data in that person's possession or control, which is stored in a computer system; and (b) any

service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control."
This provision is closely modelled on the procedural provision of 'production order' in the Budapest Convention. It also contains relevant safeguards and conditions as provided for in Article 15 of the Convention.

(c) Search and seizure of computer data

Good Practice (Jamaica): Section 18 of the Cybercrimes Act, 2015 sets out the procedure for search and seizure warrants, and provides that:
"(1) A Resident Magistrate may issue a warrant under this subsection, if satisfied by information on oath that there are reasonable grounds to suspect that there may be in place any computer material that (a) may be relevant as evidence in proving an offence; or (b) has been acquired by a person for, or in, the commission of an offence or as a result of the commission of an offence.

(2) A warrant under subsection (1) shall authorise a constable, with such assistance as may be necessary, to enter the place specified in the warrant to search for and seize the computer material". The definition of 'computer material' in this Act includes computer data.

This provision is closely modelled on the procedural provision of 'search and seizure of stored computer data' in the Budapest Convention. It also contains relevant safeguards and conditions as provided for in Article 15 of the Convention.
(d) Real-time collection of traffic data

Good Practice (Saint Vincent and the Grenadines): Section 22 of the Cybercrime Act, 2016 sets out the requirements for a real-time collection of traffic data. It provides that

"(1) A Judge, if satisfied on an ex parte application by a police officer that there is reasonable ground to believe that traffic data associated with a specified communication is reasonably required for the purpose of a criminal investigation or criminal proceedings, may order a person in control of the traffic data to – (a) collect or record traffic data associated with a specified communication during a specified period; or (b) permit and assist a specified police officer to collect or record that data.

(2) A Judge, if satisfied on an ex parte application by a police officer that there is reasonable ground to believe that traffic data is reasonably required for the purpose of a criminal investigation, may authorize a police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means."

This provision is closely modelled on the procedural provision of 'real-time collection of traffic data' in the Budapest Convention. It also contains relevant safeguards and conditions as provided for in Article 15 of the Convention.

(e) Interception of content data

Good Practice (Ghana): Sections 73 and 74 of the Cybersecurity Act 2020 set out the procedure and requirements for the application and issuing of a warrant for the interception of content data. Section 73 requires that a designated officer apply to the High Court for an interception warrant to collect or record content data, and this application must demonstrate that there are reasonable grounds to authorise the warrant connected with a particular person or premise under investigation for the purposes of national security, prevention or detection of a serious offence, etc. The application must also explain the rationale for why the content data sought will be available and identify the type of content data and users. Section 73 further requires that the application must "(e) indicate what measures shall be taken to prepare and ensure that the content data will be procured (i) whilst maintaining the privacy of other users, customers and third parties; and (ii) without the disclosure of the data of any party not part of the investigation".

Section 74 further requires the High Court to only grant the application when they are satisfied of "the extent of interception is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution; (c) measures shall be taken to ensure that the content data is intercepted whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; and (d) the investigation may be frustrated or seriously prejudiced unless the interception is permitted".

These provisions are closely modelled on the procedural provision of "interception of content data" in the Budapest Convention. They also contain relevant safeguards and conditions as provided for in Article 15 of the Convention.

Annex 4: Expanded methodology

The most relevant human rights impacted by cybercrime legislation are the rights to privacy and freedom of expression. Article 17 of the ICCPR guarantees the right to privacy and provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence". The right to privacy includes control over one's personal property (which includes computers and other devices), control over personal information and data, and the ability to communicate with others privately. Article 19 of the ICCPR guarantees the right to freedom of expression, including the right to receive and impart information and ideas of all kinds regardless of frontiers. The right to freedom of expression encompasses the right to search for, receive and impart information, ideas and communications of all kinds, through any media (and therefore online as well as offline).

As is well-established under international human rights law, any measure which interferes with either the right to privacy or the right to freedom of expression will amount to a breach of those rights unless it can be justified. In order to be justified, any restriction must meet a three-part test, namely that (i) there is a clear legal basis for the restriction, (ii) it pursues a legitimate aim, and (iii) it is necessary and proportionate to achieve that aim.

Beyond these general human rights frameworks, the Council of Europe's Convention on Cybercrime (the Budapest Convention) provides a useful starting point for countries looking to develop cybercrime laws in a rights-respecting manner. The Budapest Convention came into force in 2004 as the first multilateral treaty on cybercrime. It seeks to harmonise national laws on cybercrime, support the investigation of these crimes, and foster international cooperation.

While taking the Budapest Convention as its starting point, this tool notes that there have been criticisms of the Convention from a human rights perspective. In particular, some have suggested that the powers that the Convention provides for law enforcement agencies to investigate cybercrime are set out broadly and not matched by sufficient safeguards to protect the rights to privacy and freedom of expression. This criticism stems, in part, from the fact that the Budapest Convention leaves it to the states which have ratified it to ensure sufficient safeguards for human rights exist within their domestic legal frameworks, rather than prescriptively detailing what those safeguards should be. As such, this tool seeks to set out more clearly what safeguards should exist in relation to relevant provisions.

In addition to the Budapest Convention, there are a range of other frameworks for cybercrime legislation that have been developed, including the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), the Commonwealth Model Law on Computer and Computer Related Crime, and three Model Laws developed by the International Telecommunication Union for different regions. While there are similarities between the provisions of these frameworks and the Budapest Convention, they also diverge in many aspects and often in ways that may result in an overall lower level of protection for human rights. As such, this tool uses the Budapest Convention as its starting point, while noting the criticisms highlighted above.