ICNL

www.icnl.org
asia@icnl.org

Summary Legal Analysis

Timor-Leste's Draft Cybercrime Law

Introduction

Timor-Leste's Parliament is considering a draft Cybercrime Law, which seeks to establish the substantive and procedural criminal provisions and the collection of electronic evidence concerning cybercrimes, as well as outline international cooperation regarding cybercrimes (Art 1). ICNL analyzed the draft Cybercrime Law and compared it to international law and best practices related to freedom of expression and the right to privacy.

This analysis does not seek to present a comprehensive analysis of draft law, but rather highlights some of the key concerns.

ICNL is concerned that the draft law may impermissibly restrict the right to privacy or other civic freedoms in the following areas. Specifically, the draft law:

- Does not always provide a judicial standard, time limits, or other safeguards for communication surveillance and the searching and seizing of computer data;
- Provides inadequate protections for whistleblowers or users who inadvertently access unauthorized systems;
- Could lead to the closure of civil society organizations, media houses, and businesses; and
- Could create different penalties for electronic crimes compared to similar non-electronic crimes.

International Law

Article 19 of the ICCPR requires State parties to guarantee the right to freedom of expression, including the right to receive and impart information and ideas of all kinds regardless of frontiers.[1] The UN Human Rights Committee has stated that, "any restrictions on the operation of websites, blogs, or any other internet-based electronic or other such information dissemination systems" must comply with Article 19.[2]

[1] Timor-Leste ratified the ICCPR in 2003.
[2] Human Rights Committee, General Comment No. 34: Article 19: Freedoms of opinion and expression, para. 43, UN Doc # CCPR/C/GC/34 (2011).

Restrictions to the freedom of expression guaranteed in Article 19 are lawful only when such restrictions pass a three-part, cumulative test.[3] According to the test:

1) the restriction must be provided by law, which is clear and accessible to everyone (i.e., adheres to principles of predictability and transparency);
2) the restriction must pursue one of the purposes set out in article 19(3) of the ICCPR, namely: (i) to protect the rights or reputations of others; (ii) to protect national security or public order, or public health or morals (principle of legitimacy); and
3) the restriction must be necessary and the least restrictive means required to achieve the purported aim (i.e., adheres to principles of necessity and proportionality).

Similarly, the right to privacy is enshrined in Article 17 of the ICCPR, "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks." The right to privacy rests on the underlying premise that individuals have a "private sphere" where they can interact free from State intervention.[4] "In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous."[5]

Although Article 17 envisages necessary, legitimate and proportionate restrictions to the right to privacy, the Special Rapporteur for Freedom of Expression (Special Rapporteur) states that the right to privacy should be subject to the same permissible limitations test as the right to freedom of movement, elucidated in the Human Rights Committee General Comment 27, paragraph 15:

(a) Any restrictions must be provided by the law;
(b) The essence of a human right is not subject to restrictions;
(c) Restrictions must be necessary in a democratic society;
(d) Any discretion exercised when implementing the restrictions must not be unfettered;
(e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims. It must be necessary for reaching the legitimate aim; and
(f) Restrictive measures must conform to the principle of proportionality, they must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected.[6]

[3] See, e.g. United Nations Human Rights Council, A/HRC/17/27, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" May 16, 2011, para. 69.
[4] See, Lord Lester and D. Pannick (eds.). Human Rights Law and Practice. London, para. 4. 82 (Butterworth, 2004).
[5] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 23.
[6] Human Rights Committee, General Comment No. 27: Freedom of Movement (Article 12), para. 15, UN Doc # CCPR/C/21/Rev.1/Add.9 (1999); United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 29.

The freedom of expression and the right to privacy are interrelated, "the right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression."[7] Limitations or restrictions to one of these rights impact the enjoyment of the other. Just as a restriction to the freedom of expression must pass the three-part cumulative test derived from ICCPR Article 19 to be lawful, a restriction to the right to privacy is only lawful if it passes the test articulated in General Comment 27.[8]

(1) Investigation standards and safeguards

Issue: The draft law requires the authorities to obtain a warrant from either a Public Prosecutor's Office or a judge before ordering the preservation of computer data (Art. 15), accessing computer data (Art. 17), searching computer data (Art. 18), seizing computer data (Art. 19), seizing emails and other electronic communications and records (Art. 20) and intercepting communications (Art. 21). However, the draft law does not specify the standard for authorizing an investigation, or limit the scope or duration of warrants/orders needed to carry-out these activities. Nor does it include adequate safeguards in relation to the use of collected data to protect the freedom of expression and privacy.

Discussion: In addition to prior judicial authorization of surveillance and investigation powers, a set of safeguards needs to be in place to ensure that the system for communication surveillance and confiscation of equipment complies with the ICCPR. "Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, and the kind of remedy provided by the national law."[9]

Judicial standard of evidence. International human rights law makes clear that the collection and retention of communications data amounts to an interference with the right to privacy.[10] In order to meet a state's international legal obligations, national legislation must "stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority."[11]

The draft law requires authorities to obtain a warrant prior to accessing information or data, or prior to searching computers and other electronic communications, except in cases of emergency, which reflects good regulatory practice. However, it does not provide the evidentiary threshold that must be proven before a judge issues a warrant. Presumably this is articulated in the Code of Criminal Procedure, but the evidentiary threshold should be clearly defined in the law and should be reasonably high to avoid violations to the right to privacy. For example, low thresholds, such as "reasonable grounds to believe," amounts to a *de facto*

[7] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 24.
[8] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 29.
[9] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 81.
[10] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, paras. 19-23.
[11] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 81

approval of law enforcement requests, which may lead or contribute to an impermissible restriction on the freedom of expression.[12] The threshold should be high enough to amount to meaningful judicial oversight.

Duration of the warrant. Warrants for the search of records should be narrow in scope and relate only to a certain, defined, and limited period of time. While these safeguards are included in Article 15, they are not included in Article 21. Article 21 permits the interception of communications upon an order from a judge which should set forth the "scope" of the communications to be intercepted, "according to the specific needs of the investigation." There is no limit for the duration of the warrant.[13] International human rights law requires that periods of interception should be limited, and not extended indefinitely, and with a continued showing of the interception's necessity.

Scope of the warrant. The amount of information that can be intercepted, searched, seized and disclosed pursuant to Articles 15-21 may violate the right to privacy because these articles do not adequately require that the scope of the warrant be specified in the judicial order for the collection of computer data, records and communications. This may result in the collection of overly broad categories of private information.

Sweeping powers to surveil broad categories of private and innocent communications is likely to lead to violations to the right to privacy. Investigatory warrants should limit the type of information surveilled to information that directly pertains to the act being investigated.

Use and disposal of the information or data. Articles 15-21 contain very few requirements that the investigative authorities must follow when carrying out the search and seizure of electronic equipment. Notably, there is no requirement that the equipment or data be returned or destroyed once the investigation and subsequent criminal case, if any, is concluded. This raises significant fears that any private data left in the authorities' hands could be exposed. In general, there should be strict procedures for ordering the examination, use, and storage of the intercepted data as well as for the destruction or erasure of intercepted data.

Recommendation: Revise Articles 15 – 26 to specify a sufficiently high legal threshold for a warrant to be issued to guarantee meaningful judicial oversight; include adequate safeguards regarding the scope and duration of these investigatory powers; and include additional requirements about the use and disposal of collected information and data.

[12] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 56.
[13] Article 21(4) states that Articles 177 and 178 of the Criminal Procedure Code will apply to the interception and record of transmissions of computer data, though these articles also do not contain a time limit as to the duration of surveillance.

(2) Intent Requirement and Protections for Whistleblowers and Human Rights Defenders

Issue: Article 6 criminalizes access of a computer system ("illegal access") and Article 7 criminalizes the interception of computer data ("illegal interception"). The access or interception becomes illegal if it done without legal permission or authorization from the relevant authority or the owner. However, Articles 6 and 7 do not include an intent element and a person violating this provision may face up to five years' imprisonment.

Discussion: The Budapest Convention on Cybercrime,[14] the only major treaty addressing cybercrimes, includes provisions requiring states to criminalize illegal access, illegal interception, and data and system interference. However, these provisions require the act to be "committed intentionally." For example, to qualify as illegal access, the access to the computer system must be without right and occur "with the intent of obtaining computer data or other dishonest intent."

Under the draft Cybercrime Law, however, someone could access or intercept data or systems without the intent to commit a crime but would nevertheless face a multi-year prison sentence. For example, a young cybersecurity student discovers a glaring coding error. Intrigued by her discovery and eager to apply her new knowledge, she explores it further with the intent to determine whether it is a security weakness. However, her exploration results in her easily hacking the website. Even if she notifies the company of the security weakness, she may face prosecution.

Similarly, whistleblowers may be provided access to or may need to access certain parts of a computer system to bring corrupt acts or human rights violations to light. While states should criminalize illegal surveillance by public or private actors, "such laws should not target whistleblowers or other individuals seeking to expose human rights violations, nor should they hamper the legitimate oversight of government action by citizens. An exception should be made for them."[15]

Recommendation: Include a requirement in Articles 6 and 7 that the illegal act be "committed intentionally" and include an exception so that individuals who inadvertently access or intercept data or systems are not liable and subject to imprisonment. Consider including a further exception for whistle-blowers who do not damage the underlying computer system or data while exposing abuses in the public interest.

(3) Potential Closure of CSOs and Media Houses

Issue: Article 11 imposes criminal liability on legal entities for cybercrimes committed "in their name and in the collective interest of the people who occupy a leadership position," and by individuals "acting under the authority" of people occupying a leadership position. This allows

[14] Timor-Leste has not yet signed the Budapest Convention on Cybercrime. However, the standards set forth in it represent an emerging minimum consensus, including among the 75 States that have signed or ratified the convention. For a list of signatories and ratifications, please see: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=DOzYeqZn.

[15] United Nations Human Rights Council, A/HRC/23/40, "Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 84.

the Timor-Leste government to shut down a business or organization if a violation of the law occurred on its premises or is committed by one of its employees or agents. This could result in the closure of a civil society organization or media company that employs a whistle-blower who exposes human rights abuses or other scandal by "illegally accessing" a computer system.

Discussion: Article 11(11) and (12) permits the temporary or permanent closure of the entity or project. This could result in the closure of media organizations, civil society organizations and other businesses, which is incompatible with the freedom of association.

Involuntary dissolution is a remedy of last resort that should be utilized only for the most serious abuses and generally after notice and an opportunity to rectify the deficiency has been given:

> *The suspension and the involuntary dissolution of an association are the severest types of restrictions on freedom of association. As a result, it should only be possible when there is a clear and imminent danger resulting in a flagrant violation of national law, in compliance with international human rights law. It should be strictly proportional to the legitimate aim pursued and used only when softer measures would be insufficient.*[16]

Every media organization, civil society organization and private entity is now in danger of being shut down if one of its employees or agents commits a criminal act. The organization is liable even if that employee was acting outside of his or her official duties. Actions by governments against associations must be proportionate and the dissolution or closing of a business, organization or other legal entity is not a proportionate response to several of the crimes outlined in the draft law.[17]

Recommendation: Revise Article 11 to ensure that civil society organizations, media houses and other businesses can only be closed when there is a clear and imminent danger resulting in a flagrant violation of the law.

[16] United Nations Human Rights Council, A/HRC/20/27, "Report of UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai" May 21, 2012, para. 75. *See*, United Nations General Assembly, A/59/401, "Report of the Special Representative of the Secretary-General on human rights defenders, Hina Jilani, in accordance with General Assembly resolution 58/178" October 1, 2004, page 23; see also: United Nations Human Rights Council, A/HRC/23/39, "Report of UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai" April 24, 2013, para. 38.

[17] See, United Nations General Assembly, A/59/401, "Report of the Special Representative of the Secretary-General on human rights defenders, Hina Jilani, in accordance with General Assembly resolution 58/178" October 1, 2004, page 23; see also: United Nations Human Rights Council, A/HRC/23/39, "Report of UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai" April 24, 2013, para. 38.

(4) Penalties for electronic crimes should be comparable to the penalties of the same crime using non-electronic means.

Issue: The draft law imposes criminal liability, including imprisonment of 1-15 years for various violations, such as computer-related forgery, computer-related fraud, illegal access, illegal interception, child pornography, and revenge porn.

Discussion: Timor-Leste's penal code presumably provides for criminal penalties for sanctions for similar crimes such as fraud, forgery, theft, extortion, child pornography, etc. Individuals should not face higher criminal sentences or fines simply because the crime is committed online.

Recommendation: The drafters should review the criminal penalties and fines set forth in the draft law to ensure they are comparable to the penalties set forth in the criminal code and other existing laws. Moreover, the criminal penalties in the draft law should be proportionate to the harm caused by the crimes at issue.

Conclusion

The draft Cybercrime Law generally, and quite properly, focuses on preventing actual criminal activity from taking place on computer systems. The draft law does, however, raise certain concerns related to the right to privacy, freedom of expression and freedom of association. By following the recommendations contained in this analysis, the draft law would more fully protect the right to privacy and civic freedoms. ICNL would be pleased to provide additional reference materials and follow-up technical assistance to support efforts to protect online freedoms in Timor-Leste.