Thailand: Computer Crime Act

January 2017

Legal analysis

Executive summary

In January 2017, ARTICLE 19 analysed the December 2016 amendment to Thailand's Computer Crime Act of 2007 (the Amended Act) for its compliance with international freedom of expression standards. The Amended Act is currently awaiting the endorsement of King Maha Vajiralongkorn. ARTICLE 19 has previously reviewed the 2007 Act and called on the Thai Government to amend it.

On the outset, ARTICLE 19 notes that it is possible for Thailand to adequately punish legitimate computer crimes with far fewer offences and much greater protections for free speech. However, as this analysis shows, the Thai authorities not only failed to bring the 2007 Act into full compliance with international human rights standards, but the Amended Act contains several sweeping additions that will only serve to expand powers that have already been aggressively used to limit freedom of speech. In particular, we are concerned that:

- The Amended Act allows the government nearly unfettered authority to restrict free speech, engage in surveillance, conduct warrantless searches of personal data, and undermine freedoms to utilize encryption and anonymity;
- Vaguely-defined enhancements to offences can multiply prison sentences by up to ten or twenty times without any requirement of serious harm;
- The Amended Act criminalises defamation and obscenity, which is *ipso facto* incompatible with Thailand's freedom of expression obligations;
- Most of the offences as written amount to strict liability crimes, without clear intentionality requirements;
- The investigatory powers force service providers to retain user data or allow for warrantless access to user communications;
- There are no provisions for a 'public interest' defence that would provide an opportunity for an accused to establish that there was no harm or risk of harm to a legitimate interest in engaging in the proscribed activity, and that the public benefit in the activity outweighed any harm;
- The Amended Act problematically establishes a five-person committee that can obtain court approval to censor content online if it offends public morals. Such a power is exceedingly broad and facially threatens to censor legitimate expression on the basis of its content;
- The Amended Act is rife with broad powers that are susceptible to abuse and could severely punish legitimate political, academic, or social expression.

ARTICLE 19 urges the drafters of the Amended Act and the relevant committees in charge of scrutinising it to address the shortcomings identified above to ensure the compatibility of the Act with international standards of freedom of expression. We stand ready to provide further assistance in this process.

Key recommendations:

- All offences of the Amended Act should be modified from strict liability offences to clearly include intentionality requirements for "dishonest" intent for their commission and for "serious" harm to result before criminal liability attaches;
- Enhancements to penalties, if included, must be less severe and limited to punishing "serious" harm to computer systems comprising critical infrastructure that is necessary

for the public safety;

- Sufficient safeguards should be included for the protection of human rights and specifically reference international standards. In particular, public interest defences should be made available to ensure that legitimate whistleblowers, journalists, researchers, and human rights defenders acting in good faith are not prosecuted under the Amended Act;
- Given the broad powers given to a Competent Official under the Amended Act, the appointment of this function must be amended to include rigorous and transparent procedures and judicial scrutiny;
- Sections 6, 7, 11, 12, 14(2-4), 16, 17, 18(1-3 and 7), 20, 21, 24, and 26 of the Amended Act should be stricken in their entirety;
- Section 8 should be amended to require that interception be done "intentionally" and with "dishonest intent" by technical means, that it apply only to the interception of "non-public" data, and that it be done "without right;"
- Sections 9 and 10 should be amended. They should both omit the term "illegally" and include a requirement of "intentionality and without right" and "dishonest intent." Section 9 should also require "serious harm" before criminal penalties attach. Section 10 should require "serious hindering without right;"
- An intentionality requirement must be added to Section 13. Moreover, all paragraphs of Section 13 that cross-reference Section 12 should be stricken and the maximum penalty provision provided in the final paragraph of Section 13 should be omitted;
- Section 14(1) should be amended: it should include intent that the fraudulent data be "considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible;"
- Section 15 should be amended to require that aiding and abetting liability only attach where an individual or entity acts intentionally to further the underlying offence. Further, the provision allowing the Minister discretion to exempt a provider from liability should be omitted;
- Section 18(4-6, 8) should be amended to provide explicit due process protections, meaningful judicial oversight, and notice provisions.

Table of contents

Introduction

In this legal analysis, ARTICLE 19 reviews the 16 December 2016 amendment to the Computer Crime Act of 2007 (the Act). The Act was unanimously amended and expanded by Thailand's Parliament and is currently awaiting the endorsement of King Maha Vajiralongkorn.

ARTICLE 19 has extensive experience in analysing cyber-crime legislation and various freedom of expression laws. For example, we have previously monitored and analysed freedom of expression legislation in Thailand, including defamation laws[1] and the original draft 2007 Computer Offences Act.[2] In October 2011, in our submission to the UN Universal Periodic Review (UPR) for Thailand, we also called for amending the Computer Crime Act to better protect the right to freedom of expression.[3] We found that existing provisions were vague, overbroad, and subject to wide interpretation by government officials, and violated the Thai Constitution in effect at the time[4] as well as international law. ARTICLE 19 expressed that the 2007 Act "severely undermines the right to freely provide and receive information on the Internet." ARTICLE 19 has also observed that the political upheaval in Thailand following the military coup in 2006 saw a surge in charges under the Act to suppress critics and political opponents.[5]

Unfortunately, we find that the expanded amendments pose even greater threats to freedom of expression than what we outlined in our earlier analysis. The changes have drawn significant attention domestically and internationally. In December 2016, over 300,000 signatures were collected by the Thai Netizen Network for an online petition protesting the new measure.[6] Prime Minister Prayuth Chan-ocha said the Amended Act was needed to control the flow of inappropriate information from abroad, particularly content that is offensive to the monarch.[7] But the existing 2007 Act has already been used to file charges against critics of the government for activity online. For instance, one critic was reportedly charged under the 2007 Act and held in secret military custody for "liking" an image on Facebook that was critical of the Prime Minister.[8]

Cyber-security is currently a central issue in Thailand. The *Bangkok Post* reported in June 2016 that businesses are very concerned about cybercrimes in light of rapid digitisation.[9] However, we believe that it is vital that Thailand's efforts to address these issues are consistent with its obligations to protect and promote freedom of expression under international law. As a state party to the International Covenant on Civil and Political Rights

[1] See, e.g. ARTICLE 19, Impact of Defamation Law on Freedom of Expression in Thailand, July 2009; see also ARTICLE 19, Memorandum on Thailand's Criminal and Civil Defamation Provisions, November 2004.
[2] ARTICLE 19, Thailand: Draft Computer Offences Act, April 2007.
[3] ARTICLE 19, Submission to the UN Universal Periodic Review of the Kingdom of Thailand, Twelfth Session of the Working Group of the Human Rights Council, October 2011.
[4] Constitution of the Kingdom of Thailand, B.E. 2550 (2007), Enacted 24 August 2007, Chapter III Section 45.
[5] The previous Thai Constitution of 2007 in Chapter III, Section 45 then stipulated that "a person shall enjoy the liberty to express his opinion [and] make speech, write, print, publicise, and make expression by other means; see ARTICLE 19, Thailand: Freedom of Expression on Trial, 31 August 2011.
[6] Petition Opposing the amended Computer Crime Act, Thai Netizen Network.
[7] Interview, Prime Minister Gen. Prayut Chan-ocha, Matichon,15 December 2016.
[8] Human Rights Watch, Thailand: Junta Critic Feared 'Disappeared', 11 December 2015.
[9] Suchit Leesa-Nguansuk, AGCS: Thailand second worst for cybercrime, Bangkok Post, 8 June 2016.

(ICCPR), Thailand must ensure that any of its laws attempting to regulate electronic and Internet-based modes of expression comply with Article 19 of the ICCPR as interpreted by the UN Human Rights Committee (HR Committee) and that they are in line with the special mandates' recommendations.

The analysis not only highlights concerns and conflicts with international human rights standards within the Amended Act but also actively seeks to offer constructive recommendations on how the Act can be improved. We explain the ways in which problematic provisions in the Amended Act can be made compatible with international standards on freedom of expression and privacy and set out key recommendations at the end of each section.

ARTICLE 19 urges the drafters of the Amended Act and the relevant committees in charge of scrutinising it to address the shortcomings identified above to ensure the compatibility of the Act with international standards of freedom of expression. We stand ready to provide further assistance in this process.

International human rights standards

The protection of freedom of expression under international law

The right to freedom of expression is protected by a number of international human rights instruments that bind states, including Thailand, in particular Article 19 of the Universal Declaration of Human Rights (UDHR)[10] and Article 19 of the International Covenant on Civil and Political Rights (ICCPR).[11]

Additionally, General Comment No 34,[12] adopted by the UN Human Rights Committee (HR Committee) in September 2011, explicitly recognises that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.[13] In other words, the protection of freedom of expression applies online in the same way as it applies offline. State parties to the ICCPR are also required to consider the extent to which developments in information technology, such as Internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[14] The legal framework regulating the mass media should take into account the differences between the print and broadcast media and the Internet, while also noting the ways in which media converge.[15]

Similarly, the four special mandates for the protection of freedom of expression have highlighted in their Joint Declaration on Freedom of Expression and the Internet of June 2011 that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the Internet.[16] In particular, they recommend the development of tailored approaches for responding to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet are unnecessary. They also promote the use of self-regulation as an effective tool in redressing harmful speech.

As a state party to the ICCPR, Thailand must ensure that any of its laws attempting to regulate electronic and Internet-based modes of expression comply with Article 19 of the ICCPR as interpreted by the HR Committee and that they are in line with the special mandates' recommendations.

Limitations on the right to freedom of expression

While the right to freedom of expression is a fundamental right, it is not guaranteed in absolute terms. Restrictions on the right to freedom of expression must be strictly and narrowly tailored and may not put in jeopardy the right itself. The determination whether a restriction is narrowly tailored is often articulated as a three-part test. Restrictions must:

[10] UN General Assembly Resolution 217A(III), adopted 10 December 1948.
[11] GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.
[12] CCPR/C/GC/3, adopted on 12 September 2011, available at http://bit.ly/1xmySgV.
[13] *Ibid*, para. 12.
[14] *Ibid*, para. 17.
[15] *Ibid*, para. 39.
[16] Joint Declaration on Freedom of Expression and the Internet, June 2011.

- Be prescribed by law: this means that a norm must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[17] Ambiguous, vague or overly broad restrictions on freedom of expression are therefore impermissible;

- Pursue a legitimate aim: exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR as respect of the rights or reputations of others, protection of national security, public order, public health or morals. As such, it would be impermissible to prohibit expression or information solely on the basis that they cast a critical view of the government or the political social system espoused by the government;

- Be necessary and proportionate. Necessity requires that there must be a pressing social need for the restriction. The party invoking the restriction must show a direct and immediate connection between the expression and the protected interest. Proportionality requires that a restriction on expression is not over-broad and that it is appropriate to achieve its protective function. It must be shown that the restriction is specific and individual to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result.[18]

The same principles apply to electronic forms of communication or expression disseminated over the Internet.[19]

Prohibiting incitement to discrimination, hostility or violence

It is also important to note that Article 20(2) ICCPR provides that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence must be prohibited by law. At the same time, inciting violence is more than just expressing views that people disapprove of or find offensive.[20] It is speech that encourages or solicits other people to engage in violence through vehemently discriminatory rhetoric. At the international level, the UN has developed the Rabat Plan of Action, an inter-regional multi-stakeholder process involving UN human rights bodies, NGOs and academia - which provides the closest definition of what constitutes incitement law under Article 20 (2) ICCPR.[21]

Terrorism and incitement to acts of terrorism

There is no universally agreed definition of terrorism under international law.[22] At the same time, UN human rights bodies have highlighted the tension between freedom of expression and counter-terrorism measures. In particular, General Comment no. 34 clearly provides:

> 46. States parties should ensure that counter-terrorism measures are compatible with paragraph 3. Such offences as "encouragement of terrorism" and "extremist activity" as well as offences of "praising," "glorifying," or "justifying" terrorism, should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interference with freedom of expression. Excessive restrictions on access to information must also be avoided. The media plays a crucial role in informing the public about acts of terrorism and

[17] HR Committee, *L.J.M de Groot v. The Netherlands,* No. 578/1994, UN Doc. CCPR/C/54/D/578/1994 (1995).
[18] HR Committee, *Velichkin v. Belarus*, No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).
[19] General Comment 34, *op.cit.*, para. 43.
[20] *C.f.* European Court, *Handyside v the UK*, judgment of 6 July 1976, para. 56.
[21] See UN Rabat Plan of Action (2012). In particular it clarifies that regard should be had to six part test in assessing whether speech should be criminalised by states as incitement.
[22] See e.g. UNODC, Frequently Asked Questions on International Law Aspects of Countering Terrorism, 2009; see also UNODC, The Use of the Internet for Terrorist Purposes, 2012, para. 49.

> its capacity to operate should not be unduly restricted. In this regard, journalists should not be penalized for carrying out their legitimate activities.

Moreover, the Johannesburg Principles on National Security, Freedom of Expression and Access to Information[23] (Johannesburg Principles), a set of international standards developed by ARTICLE 19 and international freedom of expression experts, are instructive on restrictions on freedom of expression that seek to protect national security:

- Principle 2 states that restrictions sought to be justified on the ground of national security are illegitimate unless their genuine purpose and demonstrable effect is to protect the country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force. The restriction cannot be a pretext for protecting the government from embarrassment or exposure of wrongdoing, to conceal information about the functioning of its public institutions, or to entrench a particular ideology.

- Principle 15 states that a person may not be punished on national security grounds for disclosure of information if
  - the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or
  - the public interest in knowing the information outweighs the harm from disclosure.

Further, the Tschwane Principles on National Security and the Right to Information[24] also consider extensively the types of restrictions that can be imposed on access to information.

Online content regulation

The above principles have been endorsed and further explained by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Special Rapporteur on FOE) in two reports in 2011.[25]

In the September 2011 report, the Special Rapporteur also clarified the scope of legitimate restrictions on different types of expression online.[26] He also identified three different types of expression for the purposes of online regulation:

- expression that constitutes an offence under international law and can be prosecuted criminally;
- expression that is not criminally punishable but may justify a restriction and a civil suit; and
- expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others.[27]

In particular, the Special Rapporteur on FOE clarified that the only exceptional types of

[23] Adopted on 1 October 1995. The Principles have been endorsed by the UN Special Rapporteur on FOE and have been referred to by the UN Commission on Human Rights in each of their annual resolutions on freedom of expression since 1996.
[24] The Global Principles on National Security and the Right to Information (Tschwane Principles), Open Society Justice Initiative, June 2013.
[25] Reports of the UN Special Rapporteur on Freedom of Expression, A17/27, 17 May 2011 and A/66/290, 10 August 2011.
[26] *Ibid*, para. 18.
[27] *Ibid.*

expression that States are required to prohibit under international law are child pornography, direct and public incitement to commit genocide, hate speech and incitement to terrorism.

He further made clear that even legislation criminalizing these types of expression must be sufficiently precise, and there must be adequate and effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body.[28] In other words, these laws must also comply with the three-part test outlined above. For example, legislation prohibiting the dissemination of child pornography over the Internet through the use of blocking and filtering technologies is not immune from those requirements.

Surveillance of communications

The right to privacy complements and reinforces the right to freedom of expression. The right to privacy is essential for ensuring that individuals are able to freely express themselves, including anonymously,[29] should they so choose. The mass-surveillance of online communications therefore poses significant concerns for both the right to privacy and the right to freedom of expression.

The right to private communications is strongly protected in international law through Article 17 of the ICCPR[30] that *inter alia*, states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family or correspondence. In General Comment no. 16 on the right to privacy,[31] the HR Committee clarified that the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives the ICCPR. It further stated that:

> [E]ven with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by that authority designated under the law, and on a case-by-case basis.[32]

The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that like restrictions on the right to freedom of expression under Article 19, restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test:

> Article 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under article 17.[33]

---

[28] *Ibid*, para. 22.

[29] *Ibid*, para. 84.

[30] Article 17 states: 1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2) Everyone has the right to the protection of the law against such interference or attacks.

[31] HR Committee, General Comment 16, 23rd session, 1988, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994).

[32] *Ibid.*, para 8.

[33] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009, para 17.

In terms of surveillance (within the context of terrorism in this instance), he defined the parameters of the scope of legitimate restrictions on the right to privacy in the following terms:

> States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on the showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack.[34]

The Special Rapporteur on FOE has also observed that:

> The right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of the administration of criminal justice, prevention of crime or combatting terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.[35]

Anonymity and encryption

The protection of anonymity is a vital component in protecting the right to freedom of expression as well as other human rights, in particular the right to privacy. A fundamental feature enabling anonymity online is encryption.[36] Without the authentication techniques derived from encryption, secure online transactions and communication would be impossible.

The right to online anonymity has so far received limited recognition under international law. Traditionally, the protection of anonymity online has been linked to the protection of the right to privacy and personal data. In May 2015, the Special Rapporteur on FOE published his report on encryption and anonymity in the digital age.[37] The report highlighted the following issues in particular:

- Encryption and anonymity must be strongly protected and promoted because they provide the privacy and security necessary for the meaningful exercise of the right to freedom of expression and opinion in the digital age;[38]

- Anonymous speech is necessary for human rights defenders, journalists, and protestors. He noted that any attempt to ban or intercept anonymous communications during protests was an unjustified restriction to the right to freedom of peaceful assembly under

[34] *Ibid.*, para 21.

[35] Report of the UN Special Rapporteur on Freedom of Expression, Frank LaRue, A17/27, 17 May 2011, para 59.

[36] Encryption is a mathematical "process of converting messages, information, or data into a form unreadable by anyone except the intended recipient" that protects the confidentiality of content against third-party access or manipulation; see e.g. SANS Institute, History of encryption, 2001.

[37] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye A/HRC/29/32, 22 May 2015.

[38] *Ibid,* paras 12,16 and 56.

the UDHR and the ICCPR.[39] Legislation and regulations protecting human rights defenders and journalists should include provisions that enable access to and provide support for using technologies that would secure their communications;

- Restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law.[40] Laws and policies providing for restrictions to encryption or anonymity should be subject to public comment and only be adopted following a regular – rather than fast-track – legislative process. Strong procedural and judicial safeguards should be applied to guarantee the right to due process of any individual whose use of encryption or anonymity is subject to restriction.[41]

The Special Rapporteur's report also addressed compelled 'key disclosure' or 'decryption' orders whereby a government may "force corporations to cooperate with Governments, creating serious challenges that implicate individual users online."[42] The report stipulated that such orders should be

- based on publicly accessible law;
- clearly limited in scope focused on a specific target;
- implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets; and
- only adopted when necessary and when less intrusive means of investigation are not available.[43]

Cybercrime

No international standard on cybercrime exists in the area. From the regional standards, the 2001 Council of Europe Convention on Cybercrime (the Cybercrime Convention) has been the most relevant standard.[44] Although Thailand is not a signatory to the Convention, it provides a helpful model for states seeking to develop cybercrime legislation.

The Cybercrime Convention provides definitions for relevant terms, including definitions for: computer data, computer systems, traffic data and service providers. It requires State parties to create offences against the confidentiality, integrity and availability of computer systems and computer data; computer-related offences including forgery and fraud; and content-related offences such as the criminalisation of child pornography. The Cybercrime Convention then sets out a number of procedural requirements for the investigation and prosecution of cybercrimes, including preservation orders, production orders and the search and seizure of computer data.

Finally, and importantly, the Cybercrime Convention makes clear that the above measures must respect the conditions and safeguards for the protection of human rights and liberties, consistent with the ICCPR and other applicable international human rights instruments.

---

[39] *Ibid,* para 53.
[40] *Ibid,* para 56.
[41] *Ibid,* paras 31-35.
[42] *Ibid*, para 45.
[43] *Ibid*.
[44] The Council of Europe Convention on Cybercrime, CETS No. 185, in force since July 2004. As of May 2015, 46 states have ratified the Convention and a further eight states have signed the Convention but have not ratified it.

Analysis of the Amended Act

General comments

Before laying down our specific concerns, ARTICLE 19 would like to make the following general comments about the Amended Act.

- No requirements for serious harm, and enhanced penalties: We are concerned that most of the offences do not stipulate any requirement for "serious" harm to occur before criminal liability attaches. Further, sentencing enhancements contained in the Amended Act provide for significantly increased sentences up to ten- or twenty-fold without meaningful intentionality or harm requirements. Section 12, for instance, provides that most of the Amended Act's offences can have severely increased penalties when the acts are found to be "related to the maintenance of national security, public safety and national economic security or public infrastructure serving public interest;"

- Strict liability offences: Virtually none of the offences articulate a *mens rea* requirement before criminal liability attaches, requiring merely that conduct be done "illegally." This provides little notice to individuals and causes many offences to fail to be adequately defined in law (as per the requirements of the three part test – see above). We suggest that a minimum of "dishonest" and "intentional" *mens rea* be required. We also recommend that the sentences available for offences against the confidentiality, integrity and availability of computer data and systems should be reduced to one-year maximum.[45] In addition, a harm test or "public interest defence" is not provided in the Amended Act where appropriate;

- High number of offences, including overlapping offences: We note that the Amended Act incorporates an unusually high number of computer-related offences as subsections of its offences, and we question the necessity of this approach. From a comparative perspective, we note that the Act introduces several offences that do not exist in instruments like the Council of Europe Cybercrime Convention. We suggest that the Thai legislators consider that the Cybercrime Convention contains only five such offences; whilst the UK Computer Misuse Act 1990 contains four such offences and to our knowledge there have been no concerns raised that the UK is not properly equipped to deal with cybercrime;

- Child sex abuse images: ARTICLE 19 observes that the Act, while criminalising many unnecessary activities online, does not contain any provisions on child sexual abuse images online (also referred to as "child pornography"). We note that, consistent with the recommendations of the Special Rapporteur on FOE and the Cybercrime Convention, the prevention and prosecution of "child pornography" is an important and legitimate objective. Child sexual abuse images are a type of expression that States are required to prohibit under international law.[46] Prohibition of this offence might be provided for in other Thai legislation. In any case, such an offence could be drafted tracking the definitions contained in Article 9 of the Cybercrime Convention which lays down a commonly agreed definition of offences related to "child pornography" and the Internet.

[45] *C.f.* 1990 Act 3(6).

[46] *C.f.* the May 2011 Report of the Special Rapporteur, *op.cit.*; and the Cybercrime Convention, Article 9.

- Lack of procedural safeguards for human rights protections: Procedural safeguards for human rights protections are markedly absent throughout the Amended Act. There is no reference to Thailand's obligations to uphold and protect the right to freedom of expression and other human rights protected by international law. The absence of any such provisions could threaten the entire Act's compatibility with international standards and the enforcement of human rights in this area.

Recommendations

- Offences should be modified from strict liability offences to clearly include requirements for "dishonest" intent for their commission as well as for "serious" harm to result before criminal liability attaches;
- Enhancements to penalties, if they are included, must be less severe and limited to punishing "serious" harm to computer systems comprising critical infrastructure that is necessary for the public safety;
- The Amended Act should provide sufficient safeguards for the protection of human rights and specifically reference international standards;
- Public interest defences should be made available to ensure that legitimate whistleblowers, journalists, researchers, and human rights defenders acting in good faith are not prosecuted under the Act.

Definitions

In general, ARTICLE 19 welcomes that this section sheds some light upon key operative terms of the Amended Act. In particular, we note that the definitions of computer system, computer data, and traffic data are consistent with the definitions contained in the Cybercrime Convention.

We are, however, concerned about the lack of definitions of key terms connected to the prosecution of computer-related crimes. The Amended Act does not provide a definition of "damage" or clarify that only "serious" impairment or losses should attract criminal sanctions.

Further, the Minister of Digital Economy and Society (Minister) has broad discretion to appoint a "Competent Official" who then enjoys significant police powers under the Act. Section 28 only requires officials to have "knowledge of, and expertise in, computer systems" but does not require any judicial oversight on the appointment of the officials.

Recommendations:

- The Amended Act should contain a definition of "damage" which requires "serious" impairment or losses;
- Given the broad powers given to a Competent Official under the Amended Act, his/her appointment should be amended to include rigorous and transparent procedures and judicial scrutiny.

Illegal access

Section 5 of the Amended Act criminalises "illegally" accessing a computer system

containing access prevention measures unintended for an individual's use. The section does not define what "illegally" means, does not require access measures to be circumvented, and does not carry any intentionality requirement. Hence the offence appears to be a strict liability crime.

While intentional access to a computer system without right can be a legitimate offense when it is properly defined, the vagueness of this provision fall short of international standards. ARTICLE 19 notes that the Cybercrime Convention provides for "intentionally" and suggests that access be punished where it is done with "dishonest" intent by infringing security measures. Section 5 should similarly specify that intent to gain access be "dishonest" or that there be intent to obtain computer data. Further, Section 5 should require the infringement of security measures.

ARTICLE 19 also notes that Section 7 nearly duplicates the language of Section 5, with the change of punishing accessing "computer data" rather than a "computer system." Again, from a comparative perspective, we observe that the Cybercrime Convention does not provide these as separate offences, and thus the punishment of accessing computer data can be addressed by including "intent to obtain computer data" in Section 5.

Recommendations:

- The phrase "illegally accesses a computer system for which a specific access prevention measure that is not intended for their own use is available" in Section 5 of the Amended Act should be replaced with the phrase "intentionally accesses a computer system by infringing security measures and without right;"
- Section 5 should require "dishonest intent to gain access or to obtain computer data;"
- Section 7 should be omitted for being redundant. Computer data can be addressed by adding "intent to obtain computer data" to Section 5.

Disclosure of security measures

Section 6 punishes "illegally" disclosing measures designed to prevent access to a computer system, in a manner "likely to cause damage to a third party." ARTICLE 19 begins by noting that the term "illegally" is nowhere defined and provides for no intentionality requirement, in effect making the provision a strict liability offence.

The measure as written could punish those who are carrying out legitimate activities, e.g. academic and digital security research. For instance, researchers will often test software and computer systems for vulnerabilities and bugs and post their results publicly so that flaws can be addressed. Companies often hire security consultants to test systems and publish their findings. The public dissemination of such flaws, particularly in the case of open-source software, serves to improve security and usability.

Recommendation:

- Section 6 should be stricken in its entirety.

Unauthorised interception and interference

Section 8 of the Amended Act punishes illegally eavesdropping on computer data that is "not intended for the public interest or general people's use."

ARTICLE 19 notes Section 8 does not provide for any intentionality requirement. We observe that Cybercrime Convention Article 3 which punishes illegal interception has several components not present in Section 8 of the Computer Crime Act. The Convention provides for punishing "intentionally, the interception without right, made by technical means, of non-public transmissions of computer data."

Hence, we believe that Section 8 should require "dishonest intent" and that interception be done "without right." The phrase "not intended for the public interest or general people's use" is vague and should be replaced simply with "non-public."

Sections 9 and 10 punish the interference with and damaging of computer data and systems, respectively, without requiring there to be serious damage. We observe that Section 5 of the Cybercrime Convention requires system interference to include "serious hindering without right;" and it only requires that a computer system "fails to operate normally." This is an exceedingly broad provision and could lead to severe punishment of conduct that does not actually cause harm.

Both Sections 9 and 10 of the Amended Act as written only require conduct to be done "illegally" and contain no intentionality requirement. Thus, we recommend that - at a minimum - an intentionality requirement of "intentionally, dishonestly, and without right" be added to both provisions.

Recommendations:

- Section 8 should require interception to be done "intentionally" and with "dishonest intent" by technical means, apply only to the interception of "non-public" data, and be done "without right;"
- Section 8 should replace the vague "not intended for the public interest or general people's use" with "non-public;"
- Both Sections 9 and 10 should omit "illegally" and include a requirement of "intentionality and without right" and "dishonest intent;"
- Section 9 should require "serious harm" before criminal penalties attach;
- Section 10 should be amended to require "serious hindering without right.

Punishing anonymous speech

Section 11 punishes sending data or mail while covering up the source of the data "in a manner that disturbs the other person's normal operation of their computer system." ARTICLE 19 finds that this provision is unnecessary and interferes with the ability to remain anonymous online.

As we outlined in the previous section of this analysis, anonymous speech is necessary for human rights defenders, journalists, and protestors to engage in the legitimate exercise of expression both online and offline. Punishing anonymous communications is hence a restriction on expression. As the Special Rapporteur on FOE stipulated in his 2015 Report, restrictions on anonymity must meet the three-part test of limitations to the right to freedom of expression under international law.

Here, the restriction does not achieve a legitimate purpose, and is based on a vaguely-defined harm of disturbing "normal operation" of a computer system. There is neither requirement for

dishonest intent nor a requirement for serious harm. Even if anonymous conduct online were to cause harm, it could be adequately addressed by existing provisions in the criminal code. There is no legitimate purpose in punishing, on its own, anonymous speech. Doing so serves to chill many cases where anonymous speech protects and promotes freedom of expression.

Moreover, we find it concerning that the Minister is granted unchecked power to control the nature, volume, and frequency of communications. This includes the ability to decide what causes "disturbance." The provision is a blank check to censor and control legitimate communications based on content. It is incompatible with Thailand's obligations to promote freedom of expression and should be stricken.

Finally, Section 26 problematically requires service providers to retain computer traffic data, mandating them to "retain the necessary information of the service user in order to be able to identify the service user from the beginning of the service provision." This clause would prohibit privacy-protective services and search engines which are designed not to log user information or IP-addresses. Cases where investigators require data to be retained can be handled on an individual basis involving court oversight; there is no reason for a blanket rule requiring providers to retain user data.

Recommendations:

- Section 11 should be stricken in its entirety;
- The provisions of Section 11 allowing the Minister to decide the nature, volume, and frequency of e-mails grant absolute power to control and censor communications should be stricken out in their entirety;
- Section 26's requirements of user-data retention and mandating the collection of identifying information on users should be abolished.

Enhanced penalty offences involving certain computer systems

Section 12 and its subsections provide for severe penalties of up to ten to twenty times the original offence when the offence includes certain computer systems. The examples provided for these enhancements are systems "related to the maintenance of national security, public safety and national economic security or public infrastructure serving the public interest."

ARTICLE 19 is extremely concerned that these terms are broad and not formulated with sufficient precision to enable an individual to regulate his or her conduct. They do not require any "serious" harm to occur and are vulnerable to subjective interpretation. The penalties of up to fifteen or twenty years imprisonment are unduly severe.

We believe that only "serious" impairment or losses to computer systems should face criminal sanction. This reading is consistent with international standards, including the Cybercrime Convention. The one subsection stipulating serious harm, Section 12(3), namely death without intention to kill, could be dealt with using existing offences in the criminal code relating to manslaughter and thus a separate computer crime is unnecessary.

Recommendations:

- Section 12 and its subsections should be omitted as written. At a minimum, crimes against protected systems must be narrowly defined to critical infrastructure necessary for public safety, require "serious" harm and "dishonest" intent, and carry significantly less severe penalties;

- Section 12(3) should be stricken.

Illegal devices and access codes

Section 13 of the Amended Act punishes anyone who sells or disseminates instructions to commit various other offences under the Act. The provision also provides for heightened penalties in conjunction with Section 12 for offences involving certain broadly-defined computer systems.

ARTICLE 19 is extremely concerned that Section 13 creates a strict liability offence for disseminating certain technological tools. Like many tools, technologies are dual-use and it is in the nature of technology that it can be used both for legitimate and illegitimate purposes. Most companies would know that the software they manufacture or sell could be used for dual purposes, including for the purposes of unauthorised access to computer data and systems. A standard of intent, particularly a heightened standard, must be introduced so that "intent that disseminated technology be used to commit an offence under the Act" is required in Section 13. Otherwise the provision could punish legitimate activities such as security testing. This is the same standard as required under Article 6 of the Cybercrime Convention, which highlights the need for protecting system testing in Article 6(2).

In addition, we are concerned that this provision may be used to prosecute individuals or companies producing, distributing, selling or otherwise circulating software used to break Digital Management Rights systems. DRM systems are a type of technology principally used by hardware manufacturers, publishers and copyright holders to control how digital content may be used after sale. DRM systems are controversial from a freedom of expression perspective, as the legitimacy of copyright holders exercising in perpetuity absolute control over the sharing of information is strongly contested. For example, DRM systems prevent individuals from engaging in trivial and non-commercial acts of copyright infringement such as transferring data between their own electronic devices; they can also prevent individuals from using copyrighted works in a way that is ordinarily protected by the defence of "fair use."

Recommendations:

- As written Section 13 can punish the dissemination of legitimate dual-use computer software; an intentionality requirement must be added requiring that dissemination or sale of devices, software, or data be done for the purpose of committing an offence under the Act;
- The paragraphs of Section 13 that cross-reference Section 12 to impose heightened sanctions for subjectively-defined computer systems should be stricken in accord with ARTICLE 19's comments on Section 12; and
- The maximum penalty provision provided in the final paragraph of Section 13 should be stricken entirely.

Computer forgery and fraud

Section 14 and its subsections punish a wide range of conduct:

- Subsection 1 criminalises the intentional input or alteration of inauthentic computer data in a manner that is likely to cause damage "to the public;"
- Subsection 2 punishes inputting false data "likely to damage the maintenance of national

security, public security, national economic security or public infrastructure serving public interest" or "cause panic in the public;"

- Subsection 3 punishes putting into a computer system "any computer data" which is "an offense about the security of the Kingdom or is an offense about terrorism;"
- Subsection 4 proscribes putting "obscene" data that is publicly accessible. Finally, 14(5) punishes anyone disseminating data when aware that it violates any of the aforementioned provisions.

ARTICLE 19 notes that the only offence that sets forth to proscribe legitimately criminal activity - namely computer-related forgery - is Subsection 14(1). We note favourably that 14(1) requires "ill or fraudulent intent" which is similar to the recommended intentionality under Article 7 of the Cybercrime Convention addressing forgery. However, 14(1) should be amended to remove "cause damage to the public" which is unnecessarily vague. Instead, 14(1) should include intent that the fraudulent data be "considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible."

The rest of Section 14 is highly problematic and creates several offences that are not only unnecessary but could be used to dramatically limit expression online. Subsection 14(2) is overbroad as it relies upon the same subjective language of harm discussed in Section 12, without any requirement of serious harm. Further, "cause panic" is extremely vague. 14(3) may be used to punish inputting any computer data that engages in dissent and is thus deemed to be critical of government.

Subsection 14(4) punishes the public dissemination of "obscene" data, with no definition provided for "obscene." ARTICLE 19 notes that this amounts to an illegitimate content-based restriction. Obscenity is not a form of expression that may be restricted under international law. The HR Committee has affirmed that restrictions on freedom of expression for the protection of public morals must be based on a broad understanding of what 'public morals' means.

Finally, Subsection 14(5) directly abridges freedom of expression by criminalising individuals who merely disseminate data. The punishment of such re-dissemination is a sweeping restriction on speech that does not further a legitimate government interest.

Recommendations:

- Section 14(1) should be amended to remove "cause damage to the public" which is unnecessarily vague. Instead, it should include intent that the fraudulent data be "considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible;"
- The remaining provisions of Section 14 should all be stricken.

Criminal defamation

Section 16 punishes, with up to three years' imprisonment, publicly disseminating an image that has been created or edited by electronic means which is "likely to impair the reputation of such other person or to expose such other person to hatred of contempt The paragraphs that follow punish harming the 'reputations' of deceased persons.

ARTICLE 19 notes that criminal defamation laws are inherently vulnerable to being exploited

where they are left to government authorities to enforce. For this reason, we have consistently advocated for the abolition of criminal defamation laws. The HR Committee has similarly urged all states party to the ICCPR to abolish criminal defamation laws.[47] Such laws rarely can be said to pursue a legitimate aim and be necessary and proportionate. We also note that human rights law does not recognise protection of the reputation of deceased individuals.

Moreover, we note that the Sections 16(1) and (2) allow courts to order the destruction of - and compel individuals to destroy - data that is deemed "likely to impair the reputation of such other person or to expose such other person to hatred of contempt." Individuals under 16(2) have a positive obligation to destroy data or face criminal penalty. These provisions amount to content-based censorship and go beyond what is already an illegitimate and disproportionate restriction. Section 16 should be stricken entirely.

Recommendations:

- Criminal defamation provisions in Section 16 of the Act should be abolished;
- Subsections 16(1) and 16(2) must be stricken entirely.

Procedures and investigations

The remaining sections of the Amended Act set out investigatory powers and procedures, which comprise some of the most worrisome portions of the Act. While ARTICLE 19 does not propose to conduct an exhaustive analysis of this part of the Act, we do make some important observations as they pertain to the protection of the rights to privacy and freedom of expression.

Punishment for participation in offences

Section 15 punishes any service provider who "cooperates, consents or acquiesces" to an offence under Section 14. Notwithstanding the existing problems with Section 14 as enumerated above, it also appears that a proposed intentionality requirement under Section 15 was stricken from the current version of Act. This means that service providers can potentially be held responsible for aiding and abetting computer-related forgery without any intentionality. Criminal liability may attach merely for the fact that a service provider's systems are used for forgery.

From comparative perspective, we also note that Article 11 of the Cybercrime Convention requires aiding and abetting liability to attach only where it is done "intentionally." The rest of Section 15 provides wide discretion to the Minister to exempt a service provider from liability if they cooperate with investigations, opening up the provision to become a coercive tool.

Recommendation:

- Section 15 should require that aiding and abetting liability only attach where an individual or entity acts intentionally to further the underlying offence. The provision allowing the Minister discretion to exempt a provider from liability should be omitted.

[47] HR Committee, Concluding observations on Italy (CCPR/C/ITA/CO/5); Concluding observations on the Former Yugoslav Republic of Macedonia (CCPR/C/MKD/CO/2).

Extraterritorial application
Section 17 punishes computer offences that occur outside Thailand; Section 17(1) makes Thai citizens liable for their conduct outside Thailand, and 17(2) makes non-Thai citizens liable for offences against the Thai government or Thai citizens. Given the number of offences in the Amended Act that punish online speech that offends the government, the provision would appear to criminalise any journalist, human rights organization, or other party that engages in truthful expression viewed as injurious to the reputations of government officials.

Recommendation:
- Section 17 should be stricken. Otherwise, it must be amended to ensure that both Thai and non-Thai citizens who are exercising their fundamental right to freedom of expression abroad do not face criminal penalties in Thai jurisdiction.

Arbitrary settlement process
Section 17(1) provides for a Settlement Committee appointed by the Minister that has the ability to settle cases that carry sanctions of less than two years imprisonment.

ARTICLE 19 finds this provision very problematic on due process grounds. It is up to the sole discretion of the Settlement Committee to settle a case. Section 17(1) provides no guidelines for settlement and no transparency for their decision-making process. There does not appear to be any accountability or appeals process. These characteristics provide for a settlement process highly vulnerable to being subjective and arbitrary.

Recommendation:
- Section 17(1) should be removed or amended to include transparent criteria and guidelines for the settlement process and appeals so it is not vulnerable to abuse.

Warrantless Search Power
The provisions of Section 18 allow for warrantless digital search powers accompanied by gag orders by default:
- Subsection 18(1) allows officials to compel the production of data or evidence in an "understandable form" which appears to grant an ability to compel decryption of communications.
- Subsections 18(2) and 18(3) allow officials to compel production of traffic data and user-related data without built-in privacy safeguards.
- Subsections 18(4) through 18(6) similarly allow officials to compel inspection of or production of data from individuals controlling computer data or storage equipment.
- Subsection 18(8) allows for officials to seize or attach computer systems.

We note that the judicial and privacy protections in these provisions are non-existent or minimal at best. Subsections 18(1) through 18(3) do not require any court supervision or order and simply allow officials to compel production of an enormous range of personal data, traffic, communications, and activity logs with only seven days to comply. In the cases of investigative measures under Subsections 18(4) through 18(8), Section 19 requires the official to file a petition with a court. The petition must identify a "reasonable ground" for commission of the offence and adequately describe the alleged offence and desired equipment. Notice must only be given to the owner or possessor of the computer system—not the actual user being investigated. Thus, it is possible that individuals may never receive

notice of their data being subject to search.

We also find that Section 18 falls alarmingly short of containing adequate due process protections given the reaching intrusiveness of the investigative measures it authorizes. The first three measures provide no court oversight to what is essentially a limitless digital search power. The amount of time to comply—seven days—is so short as to preclude any meaningful judicial remedy. The latter provisions, including physical seizure provisions, merely contain a "reasonable ground" standard which is a relatively low criminal burden.

Per Section 24, any computer traffic data or user data acquired under any part of Section 18 is subject to a gag order, by which its disclosure by "any person" is subject to up to two years imprisonment. It is not even clear whether this provision would even allow users a right to speak to an attorney regarding demands pursuant to Section 18.

Recommendations:

- Section 18, parts (1) through (3), and Section 24, should be omitted entirely as written, or amended to require warrants including explicit due process protections, meaningful judicial oversight, and notice provisions;
- Section 18, parts (4) through (6), and (8), should be amended to provide explicit due process protections, meaningful judicial oversight, and notice provisions.

Gag order provisions

Section 20 provides far-reaching authority for officials with approval from the Minister to file petitions for writs to stop dissemination of information, or to order the deletion of data from systems. The power to gag dissemination applies to nearly limitless information, including: any data that falls under the Act, data which "may compromise the security of the Kingdom," computer data which is connected to other criminal laws and is a "breach to the public order or moral high ground of the people," and data which is not criminal but is "deemed to be a breach to the public order or moral high ground of the people." The final category must be approved by a "Computer Data Screening Committee." The Committee is appointed by the same Minister that approves the gag order.

The suppression ability gives officials authority to compel removal or suppression, or to do it "themselves," a police power which is nowhere defined or limited.

Section 20 does not provide for any procedural protections or meaningful standards or burden of proof for officials petitioning for a writ. The laxity of the procedures is illustrated by the fact that officials can apply for such writs electronically.

These provisions amount to prior restraints on speech, which are rarely proportionate or satisfy a legitimate government aim outside exceptional circumstances. Section 20 falls far short from offering any meaningful checks or due process rights connected to these powers.

For similar reasons, ARTICLE 19 believes that Section 21 should be stricken in its entirety. It allows officials to obtain writs to prohibit the sale or dissemination of computer data, or order its destruction. As discussed in reference to Section 13, computer tools are dual-use technologies that can have many purposes, including for academic and security research. The prevention of dissemination of malicious software that is intended to cause harm with dishonest intent can be properly addressed by incorporating adequate intentionality requirements into Section 13.

We note again that Section 24 incorporates a far-reaching gag order punishing anyone who discloses data collected as part of the warrantless powers in Section 18.

Recommendations:
- Section 20 should be stricken entirely;
- Section 21 should be stricken entirely. By incorporating adequate intentionality requirements into Section 13 that punish the dissemination of harmful computer tools with dishonest intent, Section 21 will be rendered unnecessary.

Compelled decryption

ARTICLE 19 is concerned that Section 18(7) problematically allows courts broad powers to compel individuals and entities to decrypt content: specifically, it allows for orders to "decode any person's computer data or instruct any person related to the encryption of computer data to decode the computer data or cooperate with a competent official in such decoding."

We note that encryption facilitates the exercise of free expression and privacy, and restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law. It is often the case that service providers do not even possess the technical capacity to decrypt end-to-end communications that pass through their systems; such providers should not face criminal penalty or contempt if this is the case.

We recall that the 2015 report of the Special Rapporteur on FOE stipulated, in the case of orders for compelled assistance to decrypt communications, that such orders should be necessary and the least intrusive means available, based on publicly accessible law, clearly limited in scope focused on a specific target, and implemented under independent and impartial judicial authority. In the 2016 case of the US Federal Bureau of Investigation attempting to force Apple Computer to compel decryption of an iPhone device, the Special Rapporteur on FOE made a written submission to the judge reiterating the position that compelled assistance to decrypt communications raises grave concerns for freedom of expression.[48]

Recommendation:
- Section 18(7) should be stricken.

[48] David Kaye, Re: In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 ED No. CM 16 - 10 (SP), March 2, 2016.

About ARTICLE 19

ARTICLE 19 advocates for the development of progressive standards on freedom of expression and freedom of information at the international and regional levels, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the organisation publishes a number of legal analyses each year, comments on legislative proposals as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of our analyses are available at http://www.article19.org/resources.php/legal.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at legal@article19.org.